



Universidad
Carlos III de Madrid

Departamento de Informática

Ingeniería Técnica en Informática de Gestión

Proyecto Fin de Carrera

Auditoría y control de redes inalámbricas

Autor: Daniel Arnaiz Rubio

Tutor: Miguel Ángel Ramos

Leganés, Septiembre de 2015

Título: Auditoría y control de redes inalámbricas

Autor: Daniel Arnaiz Rubio

Director: Miguel Ángel Ramos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día ____ de _____ de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO

PRESIDENTE

Agradecimientos

En primer lugar quiero agradecer a mi tutor Miguel Ángel, el tiempo, la paciencia y dedicación que ha invertido para este proyecto.

A mi familia que siempre me ha apoyado y animado a terminar los estudios y este proyecto, a pesar de las dificultades.

En particular a mi padre al que le debo mi interés por el mundo de la informática, y por lo tanto mi orientación académica y laboral.

A mi esposa que tanto ha sacrificado por nuestra relación, por sus ánimos y su apoyo constante, por darle sentido a todo este esfuerzo y a la vida.

Para todos ellos es esta dedicatoria de proyecto fin de carrera, pues es a ellos a quienes se las debo por su apoyo incondicional.

Resumen

En este proyecto se realizará un estudio teórico de los diferentes tipos de redes inalámbricas que existen actualmente. Centrándose principalmente en las más habituales, las redes inalámbricas de tipo local que son las que utilizamos en casa o en el trabajo.

Estudiaremos en detalle sus características, sus diferentes posibilidades, así como sus vulnerabilidades y qué podemos hacer para conseguir una red lo más segura posible.

Además, describiremos los distintos mecanismos de control y auditoría necesarios en este tipo de redes.

Por último, se desarrollará un prototipo de herramienta de auditoría, mediante la cual una persona respondiendo a una serie de cuestiones clave puede llegar a una conclusión sobre la seguridad de una red, qué debilidades tiene y cómo afrontarlas.

Abstract

This project will be a theoretical study of the different types of wireless networks that currently exist. Focusing primarily on the most common, such as local wireless networks that are the type we use at home or at work.

Includes detailed look at vulnerabilities and what we can do to make the network as secure as possible.

Also describes the different mechanisms of control and audit requirements in such networks.

Finally, it develops a prototype audit tool by which a person answering a series of key issues can come to a conclusion on the safety of a network that has weaknesses and how to deal.

Índice general

INTRODUCCIÓN	12
1.1 JUSTIFICACIÓN Y OBJETIVOS DEL PROYECTO	13
TIPOS DE REDES INALÁMBRICAS	18
2.1 TIPOS DE REDES INALÁMBRICAS	19
2.2 WPAN (REDES INALÁMBRICAS DE ÁREA PERSONAL)	21
2.2.1 Bluetooth	23
2.3 HOMERF	30
2.3.1 Infrarrojo	32
2.3.2 ZigBee	36
2.4 WLAN (REDES INALÁMBRICAS LOCALES)	40
2.4.1 HiperLan	41
2.4.2 IEEE 802.11	42
2.5 WMAN (REDES INALÁMBRICAS DE ÁREA METROPOLITANA)	55
2.5.1 WiMax	56
2.5.2 LMDS	58
2.6 WWAN (REDES INALÁMBRICAS DE ÁREA EXTENSA)	59
REDES WLAN	61
3.1 ANTECEDENTES	64
3.2 NORMALIZACIÓN	65
3.3 VENTAJAS	66
3.4 INCONVENIENTES	67
3.5 ELEMENTOS HARDWARE	68
3.6 ARQUITECTURAS O TOPOLOGÍAS DE RED WLAN	71
3.6.1 Modo IBSS	72
3.6.2 Modo BSS	73
3.6.3 Modo ESS	74
3.6.4 Modos de actuación	75
ATAQUES A REDES WLAN	77
4.1 ATAQUES PASIVOS	79
4.1.1 Espionaje (Surveillance)	79
4.1.2 Escuchas (Sniffing)	79
4.1.3 Wardriving	79
4.1.4 Warchalking	80
4.1.5 Descubrimiento de contraseña	81
4.1.6 Descubrimiento de ESSID ocultos	81
4.2 ATAQUES ACTIVOS	84
4.2.1 Punto de acceso no autorizados/Rogue APs	84
4.2.2 Spoofing	85
4.2.3 Man in the middle	87
4.2.4 Secuestro de sesiones (Hijacking)	87
4.2.5 Denegación de servicio (DOS)/Jamming	87
MECANISMOS DE SEGURIDAD EN REDES WLAN	90
5.1 MECANISMOS DE SEGURIDAD PARA IMPEDIR ACCESO A LA RED	92
5.1.1 Autenticación	92
5.1.2 Cifrado	99
5.1.3 Control de acceso	114
AUDITORÍA	116

6.1 INTRODUCCIÓN	117
6.1.1 Auditoría en general	117
6.1.2 Auditoría informática.....	117
6.2 TIPOS DE AUDITORÍA INFORMÁTICA	118
6.2.1 Control interno.....	119
6.2.2 Auditoría interna.....	121
6.2.3 Auditoría externa	122
6.3 EL AUDITOR INFORMÁTICO	124
6.3.1 Funciones	124
6.3.2 Perfil.....	125
6.3.3 Ética.....	126
6.3.4 Métodos, técnicas y herramientas	127
6.4 PAPELES E INFORMES	133
6.4.1 De entrada.....	133
6.4.2 De salida (el Informe).....	136
SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).....	141
ISO / IEC 27001	141
7.1 DEFINICIÓN DE SGSI	142
7.2 CICLO DE MEJORA CONTINUA	143
7.3 NORMA ISO / IEC 27001	144
7.3.1 Definición.....	144
7.3.2 Estructura.....	145
7.3.3 Implementación.....	148
7.3.4 Certificación.....	154
7.3.5 Anexo A	155
CONCLUSIONES	160
8.1 CONCLUSIONES PERSONALES.....	161
8.1.1 Experiencias alcanzadas.....	161
8.1.2 Objetivos cumplidos.....	161
8.1.3 Contribución	161
8.1.4 Líneas de futuro.....	162
8.2 RECOMENDACIONES DE SEGURIDAD.....	163
8.3 CHECK LIST DE APOYO PARA LA SEGURIDAD INALÁMBRICA	169
PROTOTIPO DE APLICACIÓN.....	172
9.1 ANÁLISIS	173
9.1.1 Definición del sistema.....	173
9.1.2 Identificación del entorno tecnológico.....	174
9.1.2.1 Entorno tecnológico del usuario final.....	174
9.1.2.2 Entorno tecnológico del desarrollador	175
9.1.3 Requisitos del software	176
9.1.3.1 Requisitos funcionales	177
9.1.3.2 Requisitos de usabilidad	180
9.1.3.3 Requisitos de rendimiento.....	183
9.2 DISEÑO.....	185
9.2.1 Estructura de la aplicación.....	185
9.2.2 Check list de seguridad inalámbrica	188
9.2.2.1 Nuevo check list	188
9.2.2.2 Listado de sesiones check list	189
9.2.2.3 Resultado del check list.....	190
9.2.3 Herramientas.....	196
9.2.3.1 WarDriving	196
9.2.3.2 Escaner wifi.....	200
9.2.3.3 Medidor intensidad de señal.....	202
9.3 DETALLES DE IMPLEMENTACIÓN	203
9.3.1 Modelo.....	204

9.3.1.1 Base de datos.....	204
9.3.2 Vista.....	206
9.3.2.1 Layout.....	206
9.3.2.2 Recursos	211
9.3.2.3 Imágenes.....	212
9.3.2.4 Textos, estilos, colores y valores	212
9.3.3 Controlador.....	213
9.3.3.1 Activity.....	213
9.3.3.2 GPSTracker.....	215
9.3.3.3 Google Maps	215
9.4 PRUEBAS DEL PROTOTIPO	216
9.5 FUTURAS MEJORAS DEL PROTOTIPO.....	217
PLANIFICACIÓN Y PRESUPUESTO	218
10.1 PLANIFICACIÓN	219
10.2 PRESUPUESTO	221
10.2.1 Horas dedicadas	221
10.2.2 Coste de personal.....	222
10.2.3 Coste de software	223
10.2.4 Coste de hardware	224
10.2.5 Coste de material fungible.....	225
10.2.6 Resumen de costes.....	226
10.2.7 Plantilla de presupuesto	227
FUTURAS LÍNEAS DE INVESTIGACIÓN	228
ANEXOS.....	232
12.1 GLOSARIO DE TÉRMINOS	233
12.2 BIBLIOGRAFÍA.....	245

Capítulo 1

Introducción

1.1 Justificación y objetivos del proyecto

El uso cada vez más habitual de las redes inalámbricas, tanto en el ámbito personal como en el empresarial, nos presenta un nuevo escenario en el mundo de las redes y la transmisión de datos.

Usar el aire como medio de transmisión presenta una serie de nuevas amenazas y problemáticas que se unen a las de las redes cableadas ya conocidas anteriormente.

Además, algunos factores que a priori parecen jugar a favor de este tipo de tecnología, como son su bajo coste económico y su facilidad de implantación, no siendo necesario tener conocimientos específicos de redes ni de seguridad, ha provocado que exista un gran porcentaje de redes que presentan innumerables vulnerabilidades.

El propósito de este proyecto es estudiar estas nuevas vulnerabilidades y proponer posibles soluciones, ya que el autor considera que el principal problema es que esta implantación no ha llevado consigo un estudio a fondo de las medidas de seguridad necesarias, de las nuevas amenazas que han surgido, y de cómo protegerse ante ellas.

Los principales objetivos de este proyecto son:

- Entender cada tipo de red, sus posibilidades de configuración, así como sus debilidades y fortalezas.
- Saber identificar las vulnerabilidades de las redes en las que trabajamos, y qué podemos hacer para mejorar su seguridad.
- Proporcionar una herramienta para la auditoría y el control de las redes inalámbricas.

Por otro lado, con este proyecto se pretenden una serie de objetivos secundarios:

- Concienciar al lector de la necesidad de seguir al día en el conocimiento de la seguridad y vulnerabilidades de las redes inalámbricas.
- Destacar la importancia de las auditorías y controles de seguridad, así como las políticas de seguridad y calidad.

Índice de figuras

FIGURA 1. CLASIFICACIÓN DE LAS REDES INALÁMBRICAS.....	20
FIGURA 2. LOGOTIPO DE BLUETOOTH	23
FIGURA 3. PROTOCOLOS BLUETOOTH	24
FIGURA 4. PERFILES BLUETOOTH.....	25
FIGURA 5. TOPOLOGÍA PUNTO A PUNTO	26
FIGURA 6. TOPOLOGÍA PICONET.....	26
FIGURA 7. TOPOLOGÍA SCATTER-NET	27
FIGURA 8. LOGOTIPO DE HOMERF	30
FIGURA 9. ESPECTRO ELECTROMAGNÉTICO	33
FIGURA 10. MODELO DE CAPAS IRDA	34
FIGURA 11. IEEE 802.11 MODELO OSI	42
FIGURA 12. DIAGRAMA DE LA CAPA FÍSICA DEL 802.11	46
FIGURA 13. COMPARATIVA ESTÁNDARES IEEE 802.11	51
FIGURA 14. LOGOTIPO WiMAX	56
FIGURA 15. COMPARATIVA ESTÁNDARES WiMAX	57
FIGURA 16. TOPOLOGÍAS DE RED WLAN. IBSS	72
FIGURA 17. TOPOLOGÍAS DE RED WLAN: BSS O INFRAESTRUCTURA	73
FIGURA 18. TOPOLOGÍAS DE RED WLAN: ESS	74
FIGURA 19. LENGUAJE WARCHALKING	80
FIGURA 20. ESCANEEO PASIVO	82
FIGURA 21. ESCANEEO ACTIVO	83
FIGURA 22. MECANISMO DE AUTENTICACIÓN.....	93
FIGURA 23. SISTEMA DE AUTENTICACIÓN ABIERTA	94
FIGURA 24. SHARED KEY: CLAVE COMPARTIDA	95
FIGURA 25. AUTENTICACIÓN EAP	96
FIGURA 26. GENERACIÓN CLAVE WEP.....	100
FIGURA 27. CIFRADO WEP. CÁLCULO DE CRC.....	101
FIGURA 28. CIFRADO WEP. SELECCIÓN DE CLAVE	101
FIGURA 29. CIFRADO WEP. IV + CLAVE.....	101
FIGURA 30. CIFRADO WEP. CIFRADO DEL PAYLOAD	102
FIGURA 31. CIFRADO WEP. TRAMA CIFRADA	102
FIGURA 32. DESCIFRADO WEP. DESCIFRADO DEL PAYLOAD.....	103
FIGURA 33. PAQUETE CIFRADO TKIP	109
FIGURA 34. CIFRADO TKIP	109
FIGURA 35. CIFRADO CCMP	112
FIGURA 36. CICLO PDCA.....	143
FIGURA 37. ISO / IEC 27001:2013.....	144
FIGURA 38. CICLO PDCA EN ISO/ IEC 27001:2013	147
FIGURA 39. CICLO PDCA EN ISO/ IEC 27001:2013	154
FIGURA 40. PROTOTIPO PREGUNTAS	188
FIGURA 41. PROTOTIPO RECOMENDACIONES.....	190
FIGURA 42. PROTOTIPO WARDRIVING.....	196
FIGURA 43. PROTOTIPO WARDRIVING OPCIONES	197
FIGURA 44. PROTOTIPO WARDRIVING MAPA	199
FIGURA 45. PROTOTIPO ESCÁNER	201
FIGURA 46. PROTOTIPO INTENSIDAD DE SEÑAL	202
FIGURA 47. MODELO VISTA CONTROLADOR EN ANDROID.....	203
FIGURA 48. MODELO E-R. SESIONES CHECK LIST.....	205
FIGURA 49. MODELO E-R. SESIONES WARDRIVING	205
FIGURA 50. ACTIVITY_MAIN.XML	207
FIGURA 51. CHECKLIST_CUESTIONARIO.XML	208
FIGURA 52. CHECKLIST_CUESTIONARIO.XML	209
FIGURA 53. CHECKLIST_RESULTADO.XML	210

FIGURA 54. RECURSOS. TEXTOS, ESTILOS Y VALORES.....	212
FIGURA 55. FLUJOGRAMA DE UN ACTIVITY	214
FIGURA 56. PLANIFICACIÓN	219
FIGURA 57. DIAGRAMA GANTT	220

Capítulo 2

Tipos de redes inalámbricas

El propósito de este capítulo es introducir el proyecto en el ámbito de las tecnologías inalámbricas mediante una visión de los diferentes tipos de redes existentes.

2.1 Tipos de redes inalámbricas

En los últimos años, han aparecido una gran variedad de tecnologías dentro del mundo inalámbrico, resultando en una gran diversidad de modelos de red, y a su vez, apareciendo múltiples posibilidades para su clasificación, ya sea según su cobertura, velocidad, tecnología, aplicaciones, etc.

Sin embargo, la clasificación más habitual está determinada según su cobertura en cuatro grandes grupos:

- **Redes inalámbricas de área personal.** Comúnmente denominadas WPAN por su acrónimo de la expresión en inglés *Wireless Personal Area Network*. El rango de estas redes normalmente es de unos pocos metros y su uso es completamente personal. Las tecnologías de este tipo de red están recogidas bajo el estándar IEEE 802.15, la más conocida es la Bluetooth.
- **Redes inalámbricas de área local.** También conocidas como WLAN (*Wireless Local Area Network*). Cubren distancias de 10 a 100 metros. Sus principales tecnologías son las variantes del estándar IEEE 802.11, que comúnmente conocemos como wifi (proveniente de la marca comercial **Wi-Fi**).
- **Redes inalámbricas de área metropolitana.** Conocidas como WMAN (*Wireless Metropolitan Area Network*). Son utilizadas cuando el área a cubrir es lo suficientemente extensa que las redes de área local no alcanzan, por ejemplo ciudades enteras. Su principal tecnología es WiMax (IEEE 802.16).
- **Redes inalámbricas de área extensa.** Denominadas WWAN (*Wireless Wide Area Network*). Son las de mayor alcance, siendo su rango de cobertura desde los 100 km hasta unos 1000 km. Un ejemplo de este tipo de red son los teléfonos móviles y sus principales tecnologías son GSM

(Global System for Mobile Communication), GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunication System) y LTE (Long Term Evolution).

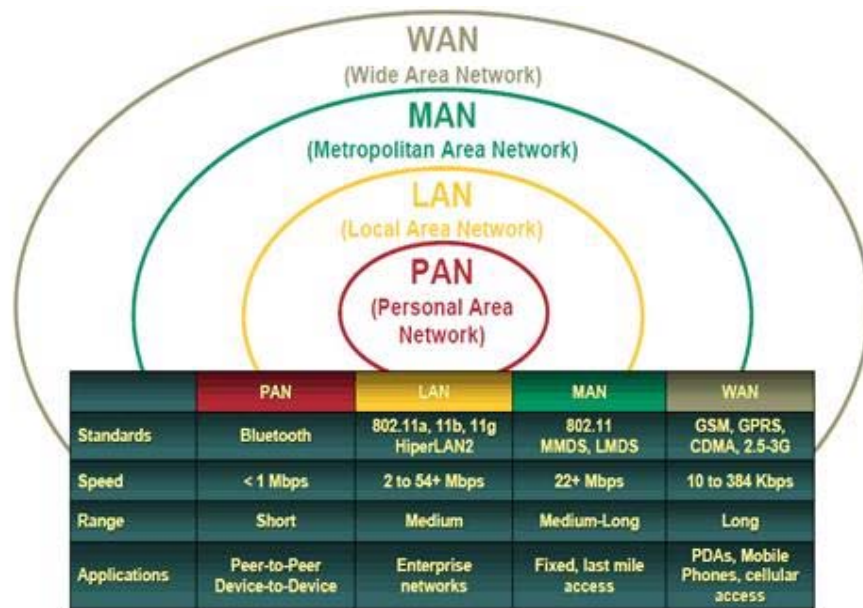


Figura 1. Clasificación de las redes inalámbricas

En este proyecto, nos vamos a centrar principalmente en los tipos de redes más utilizados y que son más accesibles para el uso particular y el mundo empresarial. Estas son las redes de área personal y sobre todo las redes de área local.

A continuación estudiaremos, con más detalle, para estos tipos de red, sus características principales, tecnologías utilizadas, ventajas e inconvenientes, debilidades y fortalezas, así como sus usos más habituales.

2.2 WPAN (Redes inalámbricas de área personal)

Las redes inalámbricas de área personal, más conocidas como WPAN por sus siglas en inglés *Wireless Personal Area Network*, son redes de corto alcance que cubren un área máxima de algunas pocas decenas de metros. Su uso más habitual es conectar punto a punto los diferentes dispositivos portátiles personales o periféricos (por ejemplo, impresoras, teclados y hasta electrodomésticos) sin la necesidad de utilizar cables.

La principal ventaja de este tipo de comunicación es que no requiere de altos índices de transmisión de datos lo cual resulta en un bajo consumo de energía. Este bajo consumo, hace de esta tecnología la más adecuada para su uso en dispositivos móviles que funcionan con baterías de poca duración.

Las tecnologías más comunes en las redes inalámbricas de área personal son:

- **Bluetooth:** Creada por Ericsson en 1994 y es la tecnología principal de las redes inalámbricas de área personal. Su alcance de entre 10 a 100 metros dependiendo del transmisor utilizado y su velocidad de 1 Mbps. Fue considerada la base de partida para desarrollar el estándar IEEE 802.15, y posteriormente clasificada dentro del 802.15.1. Su principal ventaja es el bajo consumo de energía necesario para realizar las transmisiones, algo que resulta idóneo para su aplicación en dispositivos de poco tamaño.¹
- **HomeRF (*Home Radio Frequency*):** Lanzada en 1998 por HomeRF Working Group (que incluye a los fabricantes Compaq, HP, Intel, Siemens, Motorola y Microsoft, entre otros). Su rango es superior al del Bluetooth llegando a un alcance máximo de entre 50 y 100 metros, y una velocidad

¹ Introducción a la tecnología Bluetooth [En línea] Disponible en <http://es.kioskea.net/contents/bluetooth/bluetooth-intro.php3>

de 10 Mbps. Este estándar fue abandonado en Enero de 2003 debido a que los fabricantes de procesadores se decantaron por utilizar la tecnología Wi-Fi en las placas a través de Centrino que incluyó un adaptador wifi y un microprocesador en un único componente.²

- **Infrarrojos:** Permite realizar la comunicación entre dos nodos. Esta tecnología se usa comúnmente en los diferentes aparatos electrónicos del hogar (como por ejemplo los controles remotos). Su principal desventaja es que debe existir visión directa entre los dispositivos para poder realizar la comunicación, además las ondas de luz pueden producir interferencias. En 1993 se fundó irDA (*Infrared Data Association*), la cual agrupa a más de 150 miembros, mediante la cual se estableció este estándar especificando la forma de transmisión y recepción de datos por medio de los rayos infrarrojos.³
- **Zigbee:** Fue creada para satisfacer la necesidad del mercado de un estándar de redes inalámbricas que fuera seguro, de bajo consumo, económico y con bajas velocidades de transmisión de datos. Está basado en el estándar IEEE 802.15.4 y especifica un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo. Dada la particularidad de sus características, diferentes de las otras tecnologías del ámbito de las redes personales, como su topología en malla de red, su facilidad de integración en pequeños aparatos electrónicos del hogar, su bajo consumo, etc., es ideal para su aplicación en el cada vez más utilizado mundo de la domótica. Funciona en la banda de frecuencia de 2,4 GHz, y puede alcanzar una velocidad de transferencia de hasta 250 Kbps con un alcance máximo de unos 100 metros.⁴

² HomeRF [En línea] Disponible en <http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/Oct06Marzo07/ComInalam/TRabajos/Trabajo2/Proyecto2%20grupo5.pdf>

³ *Infrared Data Association* [En línea] Disponible en <http://www.irda.org/>

⁴ A fondo Zigbee [En línea] Disponible en <http://www.domodesk.com/content.aspx?co=97&t=21&c=47>

2.2.1 Bluetooth

En 1994, Ericsson inició investigaciones con el fin de reemplazar el cableado existente entre teléfonos móviles, PDAs, ordenadores portátiles y sus accesorios. Estas investigaciones concluyeron con la implementación de la tecnología para las redes inalámbricas de área personal denominada Bluetooth que permite la transmisión de voz y datos sin cables entre dispositivos en un radio de corto alcance.

Como curiosidad, el nombre elegido por Ericsson para esta tecnología fue tomado del rey nórdico Harald Blåtand, cuya traducción al inglés es Harold Bluetooth. Este rey fue conocido por sus grandes dotes comunicativas, consiguiendo la unión de los países nórdicos y la conversión al cristianismo de la hasta entonces tradicional sociedad vikinga.



Figura 2. Logotipo de Bluetooth

En febrero de 1998, Ericsson se une a otros cuatro de los más importantes fabricantes de dispositivos móviles y computadoras portátiles (Nokia, IBM, Toshiba e Intel) formando el grupo denominado SIG (*Special Interest Group*) con el fin de crear una especificación global para la conectividad sin cables de corto alcance.

El Bluetooth SIG progresivamente fue adhiriendo nuevos miembros, como las compañías 3Com, Axis Communications, Compaq, Dell y Motorola entre otros, llegando en la actualidad a más de 2500 empresas.

¿Qué es Bluetooth?

Bluetooth como se denomina comúnmente, o IEEE 802.15.1, es un estándar compuesto por dos capítulos, en uno de ellos se describen los protocolos y las especificaciones técnicas, y en el otro los perfiles para las aplicaciones.

- **Protocolos:** Describen como se han de realizar las tareas básicas como señalización, gestión del enlace y el servicio de descubrimiento.

Las aplicaciones pueden operar con distintos protocolos; sin embargo, las capas más bajas son comunes a todos ellos. Como se observa en la figura a continuación, estas son la capa de banda base y la interfaz de radio.

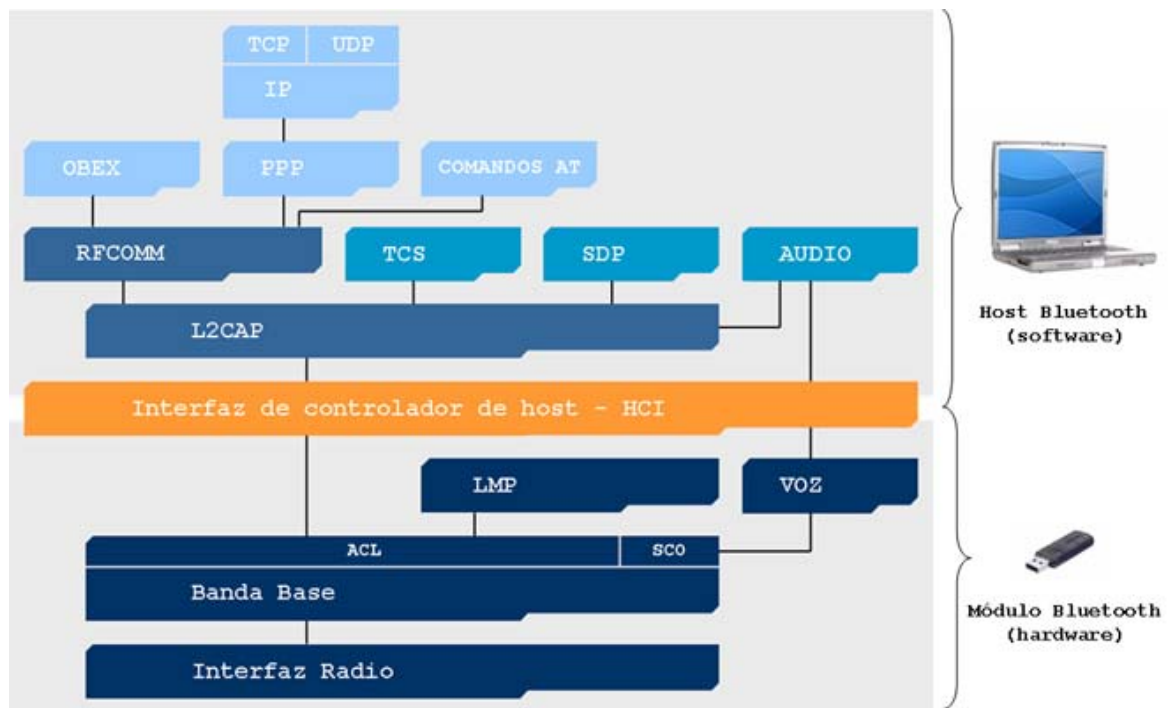


Figura 3. Protocolos Bluetooth

- **Perfiles:** Describen los comportamientos que los dispositivos pueden utilizar para comunicarse, es decir, los tipos de servicios que ofrece un dispositivo Bluetooth. Se definen cuatro perfiles genéricos que contienen la especificación de otros perfiles más específicos para modelos de uso:
 - Perfil de Acceso Genérico (**GAP, Generic Access Profile**)
 - Perfil de Puerto Serie (**SPP, Serial Port Profile**)
 - Perfil de Aplicación de Descubrimiento de Servicios (**SDAP, Service Discovery Application Profile**)
 - Perfil Genérico de Intercambio de Objetos (**GOEP, Generic Object Exchange Profile**).



Figura 4. Perfiles Bluetooth⁵

⁵ [En línea] <https://elviradev.wordpress.com/2007/12/17/perfiles-bluetooth/>

Topologías Bluetooth

Los dispositivos que utilizan la tecnología Bluetooth se comunican entre sí de forma independiente sin la necesidad de ningún hardware adicional.

Esto simplifica bastante las posibles topologías, que se clasificarán según el número de nodos conectados en la red, así como la función de cada nodo.

- **Topología punto a punto:** Define la conexión directa entre dos nodos, actuando uno como maestro y otro como esclavo.

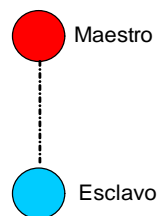


Figura 5. Topología punto a punto

- **Topología Piconet:** En este tipo de red existe un nodo maestro y hasta siete esclavos, siendo las conexiones necesariamente maestro-esclavo, no pudiendo establecer comunicación esclavo-esclavo directamente sin pasar por el nodo maestro.

Solo pueden existir ocho nodos activos al mismo tiempo, pero podrían existir más nodos dentro de la *piconet* en estado estacionario.

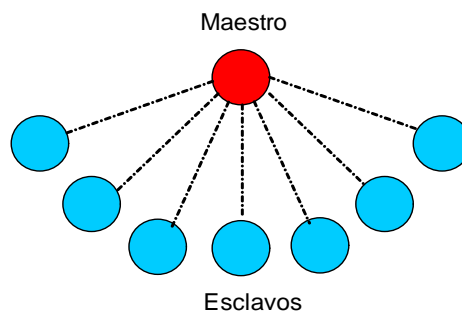


Figura 6. Topología Piconet

- **Topología Scatter-net:** Se conoce como *Scatter-net* a la unión de varias *piconet*. Esta unión entre *piconet* se puede realizar de dos formas según la actuación del nodo que las comunica:
 - **Maestro-Esclavo:** Un nodo que actúa como maestro en una red, es a su vez esclavo para otro maestro. Sin embargo un mismo nodo no puede ser maestro de más de una *piconet* a la vez.
 - **Esclavo-Esclavo:** Un mismo nodo actúa como esclavo para dos maestros diferentes.

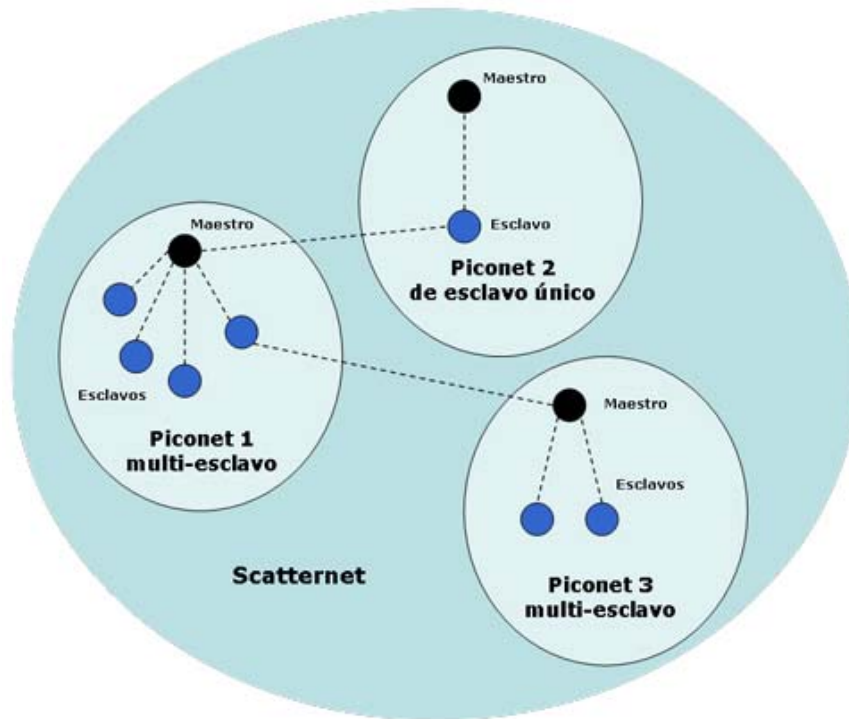


Figura 7. Topología Scatter-net

Funcionamiento Bluetooth

Un sistema con tecnología Bluetooth consiste en emisor y receptor de radio frecuencia que opera en la banda ISM de 2,4 GHz, la cual está disponible en todo el mundo, garantizando así el carácter global de esta especificación, además de ser una frecuencia que no necesita licencia.

Utiliza técnicas de modulación basadas en saltos de frecuencia FHSS (*Frequency Hopping Spread Spectrum*) que consiste en dividir la banda de frecuencia en 79 canales de 1 MHz de longitud y realizar 1600 saltos por segundo. Esto permite reducir la interferencia y comunicarse en áreas donde existe una gran actividad electromagnética.

Los datos se transmiten soportando velocidades de 1 Mbps y de hasta 2 o 3 Mbps en sistemas con EDR (*Enhanced Data Rate*).

Además de los canales de datos, dispone de tres canales de voz a 64 Kbps. Para la transmisión de voz por estos canales se utiliza el método CVSD (*Continuous Variable Slope Delta Modulation*) que permite que la voz sea perfectamente audible incluso en situaciones con ruido.

Seguridad Bluetooth

La seguridad en la tecnología Bluetooth viene especificada en el Perfil de Acceso Genérico (GAP, *Generic Access Profile*) el cual define los procedimientos para descubrir dispositivos, además de los procedimientos de gestión de enlace para establecer una conexión entre dos dispositivos. En él se definen tres mecanismos de seguridad:

- **Modo no seguro:** El dispositivo no inicia ningún procedimiento de seguridad.
- **Seguridad a nivel de servicio:** Se inician los procedimientos de seguridad una vez que la comunicación ya ha sido establecida.
- **Seguridad a nivel de enlace:** Se realizan los procedimientos de seguridad antes de que la comunicación se haya establecido.

Además a nivel de dispositivo existen dos niveles de seguridad en el acceso a los servicios:

- **Dispositivo de confianza:** Tienen acceso sin restricciones a todos los servicios.
- **Dispositivo sin confianza:** El acceso a los servicios está limitado.

A su vez, para los servicios existen tres niveles de seguridad:

- **Servicios que requieren autorización y autenticación:** Solo tendrán acceso los dispositivos que sean de confianza.
- **Servicios que sólo requieren autenticación:** Puede acceder a ellos cualquier dispositivo que se haya autenticado.
- **Servicios abiertos a todos los dispositivos.**

2.3 HomeRF

En 1998, HomeRF fue diseñado por el Grupo de Trabajo HomeRF (*HomeRF Working Group*). Se basa en la especificación del Protocolo de Acceso inalámbrico compartido (SWAP), que permite a los ordenadores, periféricos, teléfonos inalámbricos y otros dispositivos electrónicos compartir datos y comunicarse dentro del hogar, sin las dificultades y costes de tener que tender nuevos cables.



Figura 8. Logotipo de HomeRF

Finalmente en 2003, el grupo de trabajo HomeRF fue disuelto.

Entre los miembros que formaron parte de este grupo se encuentran compañías líderes en la industria de ordenadores, comunicaciones, electrónica, software y semiconductores. Como Toshiba, Compaq, Ericsson, Motorola, HP, IBM, Intel, Microsoft, Philips, Harris Semiconductor, National Semiconductor, Rockwell y Samsung.

¿Qué es HomeRF?

HomeRF está basada en la especificación SWAP (*Shared Wireless Access Protocol*) y fue creada como solución de redes inalámbricas para hogares y domótica.

SWAP es una especificación abierta que permite a los ordenadores, periféricos, teléfonos inalámbricos y otros dispositivos electrónicos compartir y comunicar

voz y datos dentro y alrededor de la casa, sin las complicaciones y gastos de tener que tender nuevos cables.⁶

Soporta tanto servicios enfocados a transmisión de datos, tipo TCP/IP, como protocolos para voz tipo DECT/GAP.

Funcionamiento HomeRF

El estándar HomeRF, al igual que Bluetooth, utiliza saltos de frecuencia FHSS sobre la banda ISM de 2,4 GHz.

La especificación 2.0 soporta velocidades de transmisión de datos de hasta 10 Mbps, siendo bastante más altas que la especificación inicial que no superaba los 1.6 Mbps.

⁶ [En línea] Disponible en

http://www.cordobawireless.net/portal/descargas/Wireless_intro.pdf

2.3.1 Infrarrojo

En 1993 se funda la asociación de datos por infrarrojos IrDA (*InfraRed Data Association*), la cual define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojos.

En la actualidad, hay más de 150 firmas en esta organización, entre ellas HP, IBM, Acer y otros.

¿Qué es Infrarrojo?

La radiación infrarroja (IR) es la tecnología usada por los mandos a distancia de televisores, cadenas de sonido, etc.

Funciona enviando comandos en un único sentido, a baja velocidad y a una distancia máxima de 9 metros, siempre teniendo que tener visión directa entre emisor y receptor.

En la versión inicial, IrDA 1.0, la velocidad de transferencia de datos ascendía a 115 Kbps en un radio de acción de 1 metro. Sin embargo, en 1996 se adoptó una extensión, el IrDA 1.1, consiguiendo aumentar la velocidad máxima de transmisión hasta los 4 Mbps (35 veces superior a la versión 1.0).

En la figura a continuación se puede ver donde se sitúa el infrarrojo en el espectro electromagnético según su longitud de onda:

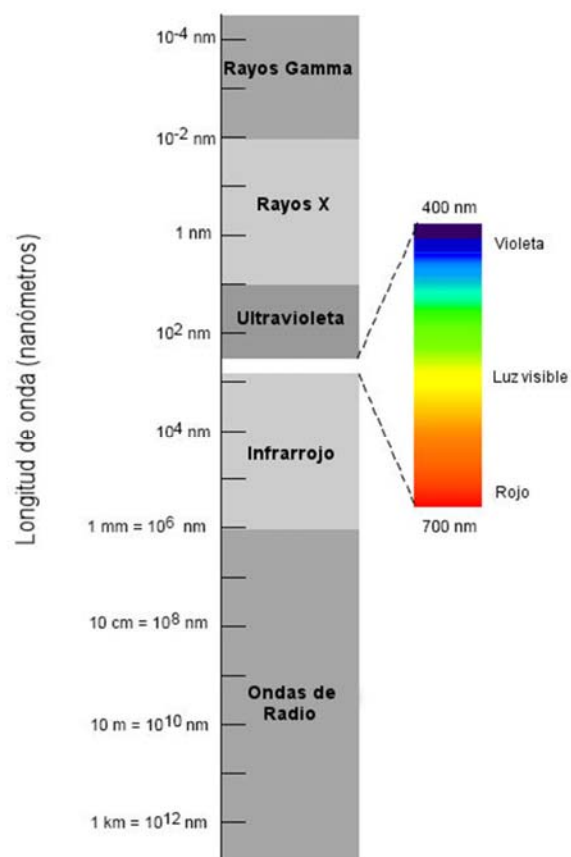


Figura 9. Espectro electromagnético⁷

⁷ Curso de Radioastronomía básica de Jet Propulsion Laboratory (JPL). marzo 27, 2009 | By Astro Tiare

Estructura

El estándar IrDA define la siguiente organización de capas

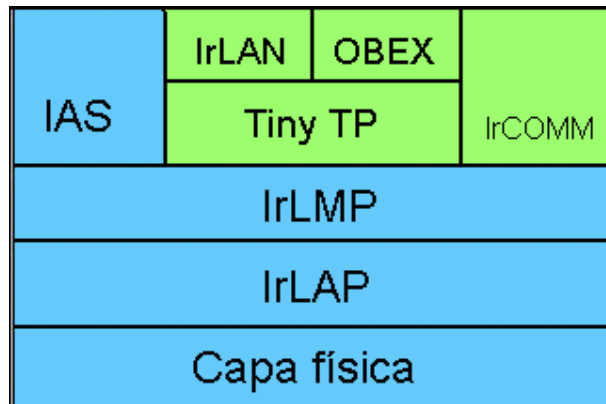


Figura 10. Modelo de capas IrDA⁸

Se establecen como obligatorios los protocolos marcados en azul, siendo los marcados en verde opcionales en su implementación.

Protocolos

- **IrPHY (*IrDA Physical Signaling Layer*):** La capa física establece la distancia máxima, la velocidad de transmisión y el modo en el que se transmite la información.

La comunicación funciona en modo bidireccional pero no simultáneo (*half duplex*) puesto que el receptor es cegado por la luz del transmisor haciendo imposible recibir y transmitir al mismo tiempo. Sin embargo, dos dispositivos pueden simular una conexión *full duplex* invirtiendo la comunicación rápidamente.

⁸ [En línea] http://es.wikipedia.org/wiki/Infrared_Data_Association

- **IrLAP (*IrDA Infrared Link Access Protocol*):** Es el protocolo de acceso al enlace, se utiliza para el descubrimiento de dispositivos cercanos y el establecimiento de conexiones confiables entre ellos.

Controla que los diferentes dispositivos no choquen entre sí en una comunicación múltiple.

- **IrLMP (*IrDA Infrared Link Management Protocol*):** Este protocolo es utilizado para el descubrimiento de servicios cercanos, no hay que confundir con el nivel anterior IrLAP, el cual ofrecía descubrimiento de dispositivos y no de servicios concretos. Además controla el flujo de datos y ofrece multiplexado garantizando el uso de varios canales a nivel IrLAP.
- **IAS (*Information Access Service*):** Actúa como unas páginas amarillas para un dispositivo.
- **Tiny TP (*IrDA Transport Protocols*):** Define como se han de manejar los canales virtuales entre dispositivos, realizando el tratamiento de división y reensamblado de paquetes, así como corrección de errores por paquetes perdidos.
- **IrCOMM:** Utilizado para adaptar IrDA al método de funcionamiento de los puertos serie y paralelo.
- **IrLan:** Permite establecer conexiones entre ordenadores portátiles y redes locales de oficina.
- **IrOBEX (*IrDA Object Exchange Protocol*):** Define una serie de comandos para permitir el intercambio de datos entre dispositivos.

2.3.2 ZigBee

A finales de 2004, el grupo de desarrollo denominado ZigBee Alliance aprobó la especificación 1.0 de este estándar, denominada comúnmente ZigBee 2004.

La segunda versión, denominada *ZigBee 2006*, fue aprobada en el 2006 como su nombre indica, y modifica la estructura utilizada hasta ese momento, dejando así obsoleta a la anterior versión.

Finalmente, en 2007 ZigBee Alliance presentó una nueva versión, denominada Pro, centrándose en la optimización de funcionalidades de nivel de red (como agregación de datos).

¿Qué es ZigBee?

Se basa en el estándar IEEE 802.15.4 el cual define una serie de protocolos de alto nivel de comunicación inalámbrica cuyo objetivo principal es su utilización con radios digitales de bajo consumo.

Está pensado para su uso en aplicaciones que no requieren una gran cantidad de envío de datos, pero que sin embargo necesitan una larga duración de la batería. Un ejemplo de este uso pueden ser sensores de control médico, industrial o la domótica.

El estándar utiliza la banda ISM (*Industrial, Scientific and Medical*) que está reservada para usos industriales, científicos y médicos; en concreto, las frecuencias de 868 MHz en Europa, 915 en Estados Unidos y 2,4 GHz en todo el mundo. Sin embargo, en la práctica, los fabricantes de dispositivos optan por utilizar la banda de 2,4 GHz, ya que es libre en todo el mundo.

Funcionamiento ZigBee

Se definen tres tipos distintos de dispositivos según su papel en la red ⁹:

- **Coordinador ZigBee (ZigBee Coordinator, ZC).** Como su nombre indica, su función es ser el coordinador de la red, esto es controlar la red así como los caminos que deben seguir los dispositivos para conectarse entre ellos. Es imprescindible que haya uno en cada red ZigBee.
- **Router ZigBee (ZigBee Router, ZR).** Interconecta dispositivos separados en la topología de la red, además de ofrecer un nivel de aplicación para la ejecución de código de usuario.
- **Dispositivo final (ZigBee End Device, ZED).** Posee la funcionalidad necesaria para comunicarse con su nodo padre (el coordinador o un *router*), pero no puede transmitir información destinada a otros dispositivos. De esta forma, este tipo de nodo puede estar dormido la mayor parte del tiempo, aumentando la vida media de sus baterías.

Como ejemplo de aplicación en Domótica, en una habitación de la casa tendríamos diversos Dispositivos Finales (como un interruptor y una lámpara) y una red de interconexión realizada con *Routers* ZigBee y gobernada por el Coordinador.

También puede plantearse una segunda clasificación de los dispositivos, dependiendo de su funcionalidad¹⁰:

- **Dispositivo de funcionalidad completa (FFD):** Dispositivo capaz de recibir mensajes en formato del estándar 802.15.4 y funcionar como

⁹ Dispositivos ZigBee http://www.ecured.cu/index.php/Dispositivos_ZigBee

¹⁰ ZigBee y sus aplicaciones

<http://www.dea.icae.upco.es/sadot/Comunicaciones/avanzadas/Zigbee%20y%20sus%20aplicaciones.pdf>

coordinador o *router*. Puede ser usado en dispositivos de red que actúen de interfaz con los usuarios.

- **Dispositivo de funcionalidad reducida (RFD):** Dispositivo con una capacidad y funcionalidad limitadas con el fin de conseguir el coste más bajo posible. Básicamente, son los sensores/actuadores de la red.

Los nodos independientemente de su modo de funcionamiento, pueden permanecer dormidos la mayor parte del tiempo, reduciendo así su consumo. Tan solo se despiertan cuando va a ser utilizado, o cada cierto tiempo, por un instante, para confirmar que sigue vivo y perteneciendo a la red. El tránsito entre los estados dormido y despierto se realiza en apenas 15 ms por lo que el servicio no se resiente.

Topologías de red

Existen tres topologías básicas:

- **Topología en estrella:** el coordinador se sitúa en el centro.
- **Topología en árbol:** el coordinador será la raíz del árbol.
- **Topología de malla:** al menos uno de los nodos tendrá más de dos conexiones.

La topología que más ventajas ofrece, y en la que basa su punto fuerte ZigBee es la topología de malla. Al tener los nodos más de dos conexiones, si un nodo del camino falla y se cae, la red puede seguir la comunicación entre todos los demás nodos. El coordinador recalculará los caminos entre nodos sin tener en cuenta al nodo caído.

Estrategias de conexión

Permite el uso de dos estrategias para la comunicación entre los dispositivos:

- **Con balizas:** Las balizas son usadas para sincronizar los dispositivos de la red, permitiendo conocer en todo momento cuándo un dispositivo puede transmitir.

El coordinador realiza envíos de mensajes a todos los dispositivos, esto se denomina balizamiento, los dispositivos de la red escuchan al coordinador, y si desea intervenir, se registra para dicho coordinador, y es entonces cuando mira si hay mensajes para él. Si tiene mensajes actúa en consecuencia, en caso contrario, el dispositivo se vuelve a dormir y se despertará de nuevo acorde al periodo de tiempo acordado por el coordinador. De la misma forma el coordinador, una vez terminado el balizamiento, vuelve a dormir.

Los intervalos de las balizas suelen variar desde los 15ms hasta los 4 minutos, dependiendo del sistema y la necesidad de ahorro de batería.

Su uso está recomendado cuando el dispositivo coordinador funciona con una batería.

- **Sin balizas:** Los dispositivos están durmiendo la práctica totalidad del tiempo, tan solo, cada cierto tiempo se despiertan para comunicarle al coordinador que siguen formando parte de la red. Cuando se dispara un evento, el dispositivo se despierta y transmite la alarma al coordinador, el cual está escuchando durante todo el tiempo.

Su ejemplo de uso más común es un sistema de seguridad, los sensores estarán durmiendo y solo se activan en caso de detectar algún evento, el cual será notificado inmediatamente a la centralita de alarma del lugar.

El dispositivo coordinador no duerme, por lo tanto, lo más habitual y recomendable es que esté conectado a la red de alimentación.

2.4 WLAN (Redes inalámbricas locales)

Las redes inalámbricas de área local, más conocidas como WLAN por sus siglas en inglés *Wireless Local Area Network*. Se denominan locales, ya que normalmente cubren distancias entre 10 y 100 metros. Trabajan en bandas de frecuencia que no necesitan licencia para operar, lo que supone una gran ventaja en cuanto al ahorro económico respecto a otras tecnologías más potentes. Esas características hacen que aunque en un principio se pensaron para el uso empresarial, ha resultado ser la tecnología ideal, también, para el uso personal.

Entre las tecnologías más comunes en las redes inalámbricas de área local se encuentran principalmente dos tipos:

- **HiperLan** (*High Performance Radio LAN*): Es un estándar del Instituto de Estándares de Telecomunicaciones Europeo (ETSI) diseñado inicialmente para competir con el IEEE 802.11b ofreciendo una mayor velocidad de transmisión.
- **IEEE 802.11**: Es un estándar internacional que especifica el uso de los niveles inferiores de la arquitectura OSI (la capa física y de enlace de datos), definiendo las normas de funcionamiento dentro de una red inalámbrica.

2.4.1 HiperLan

HiperLan es un estándar creado en 1995 por el Instituto Europeo de Telecomunicaciones ETSI. Originalmente usaba la frecuencia de 2,4 GHz, la misma que usa Bluetooth, y alcanzaba velocidades de transferencia de 1 o 2 Mbps.

En un segundo paso, abrieron una estrecha colaboración con el IEEE y el Grupo de Acceso Multimedia con Comunicaciones Móviles de Japón para rediseñar el sistema adaptándolo a frecuencias de 5 GHz, con el fin de aumentar la velocidad de transferencia de datos hasta los 55 Mbps. Consiguiendo así poder dar prioridad al tráfico de voz sobre el de datos.

Su principal ventaja es a su vez su mayor inconveniente, ya que al utilizar la frecuencia de 5 GHz, diferente a la del Bluetooth (2,45 GHz), ambas tecnologías son compatibles y pueden coexistir en el mismo dispositivo. Sin embargo, el consumo de energía sería demasiado elevado, con lo cual su uso queda muy limitado en los dispositivos móviles o portátiles.

2.4.2 IEEE 802.11

El estándar 802.11 fue publicado 1997 por el IEEE (*Institute of Electrical and Electronics Engineers*). Posteriormente adoptado en 1999 como estándar internacional conjuntamente por la ISO (*International Organization for Standardization*) y la IEC (*International Electrotechnical Commission*) bajo el nombre ISO/IEC 8802.11.

Este estándar especifica los protocolos de comunicación en redes inalámbricas. Más específicamente, define el comportamiento de los niveles inferiores del modelo OSI para este tipo de redes.

- **Capa de enlace de datos:** Define los métodos de acceso y las reglas para la comunicación entre las estaciones de la red. A su vez está compuesta por dos subcapas denominadas control de enlace lógico (LLC) y control de acceso al medio (MAC), centrándose la especificación en esta última.
- **Capa física:** Define la modulación de las ondas de radio y las características de señalización para la transmisión.

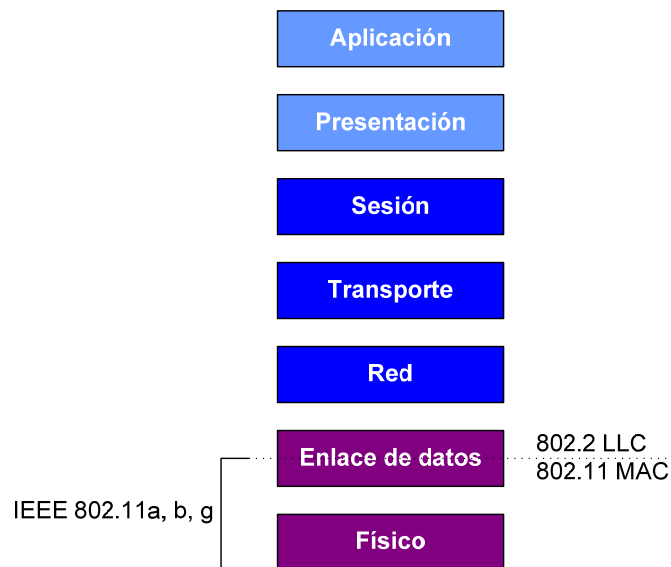


Figura 11. IEEE 802.11 Modelo OSI

El resto de protocolos del modelo OSI se utilizan en las redes inalámbricas de la misma forma que en una red cableada.

Capa de enlace de datos

El estándar IEEE 802.11 define un total de nueve servicios MAC (*Medium Access Control*):

- Seis servicios para la transmisión de paquetes (*MAC Service Data Unit*, MSDUs) entre estaciones. Los servicios son: entrega de MSDUs (*MSDU delivery*), distribución (*distribution*), integración (*integration*), asociación (*association*), reasociación (*reassociation*) y desasociación (*disassociation*)
- Tres servicios para controlar el acceso a la LAN 802.11 y para proporcionar confidencialidad a la transacción de datos. Son: autenticación (*authentication*), desautenticación (*deauthentication*) y privacidad (*privacy*).

En el protocolo MAC se diferencian tres tipos de tramas:

- **Tramas de control:** Se utilizan para controlar la comunicación y la entrega de tramas.
- **Tramas de datos:** Transportan la información a transmitir.
- **Tramas de gestión:** Se utilizan para soportar los servicios de 802.11.

Establece como método de acceso al medio lo que se llama DCF (*Distributed Coordination Function*) el cual está basado en CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*).

Además, de manera opcional, el estándar IEEE 802.11 define la técnica de coordinación llamada PCF (*Point Coordinated Function*), la cual, al ser una técnica centralizada, solo está disponible en modo infraestructura.

- **Distributed Coordination Function (DCF)**

Cuando una estación desea transmitir lo primero que hace es escuchar el canal para determinar si está libre u ocupado.

- Si se detecta como libre la estación comienza la transmisión.
- Si se detecta como ocupado, la estación espera a que el canal quede libre, y llegado ese instante, para evitar colisiones utiliza el algoritmo *backoff* aleatorio, que consiste en esperar un tiempo aleatorio antes de volver a intentar la transmisión.

Además al tratarse de un medio inalámbrico, con el fin de aumentar la fiabilidad en la entrega de paquetes se incluyen mecanismos de *acuse de recibo* y retransmisión.

Cuando una estación recibe un paquete del cual es destinatario, envía a la estación de origen una trama de *acuse de recibo* (ACK). A su vez, la estación de origen está esperando por ese ACK durante un tiempo determinado, en caso de no recibirlo inicia el proceso de retransmisión del paquete.

- **Point Coordinated Function (PCF)**

PCF alterna dos periodos de tiempo:

- Periodos con conflictos (CP: *Contention Period*): Durante los cuales las estaciones simplemente utilizan DCF.
- Periodos libres de conflictos (CFP: *Contention Free Period*): Durante estos periodos el punto de coordinación (AP) controla qué estación puede transmitir en cada momento de manera síncrona con un algoritmo Round-Robin.

En una de las evoluciones del estándar original, el IEEE 802.11e, se define una nueva función de coordinación:

- **Hybrid Coordination Function (HCF)**

Añade funciones para garantías de QoS y para permitir aplicaciones de tiempo real.

Capa física

La capa física de cualquier red define la modulación y la señalización para la transmisión de datos, más concretamente para el estándar 802.11, a priori, define tres técnicas de transmisión basadas en dos métodos:

- Infrarrojo Difuso: apenas se utiliza comercialmente.
- Transmisión Radio Frecuencia:
 - FHSS (*Frequency Hopping Spread Spectrum*)
 - DSSS (*Direct Spread Spectrum*)
 - OFDM (*Orthogonal Frequency Division Multiplexing*)

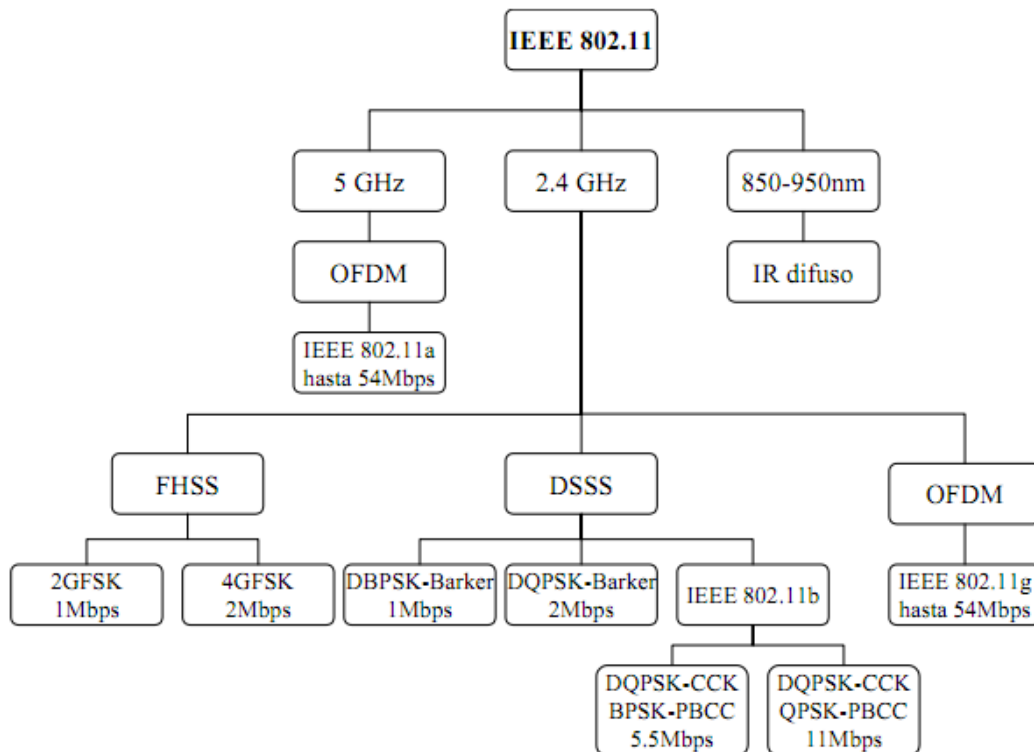


Figura 12. Diagrama de la capa física del 802.11

- **FHSS (Espectro ensanchado por salto de frecuencia)**

La tecnología de transmisión de expansión de espectro por salto de frecuencia, denominada FHSS por sus siglas de *Frequency Hopping Multiple Access*.

La señal de datos se modula sobre una señal portadora de banda estrecha que salta de forma aleatoria pero predecible de una frecuencia a otra. Para el cálculo de saltos se utiliza una función temporal sobre una amplia banda de frecuencias.

Las frecuencias de transmisión se determinan mediante un código de expansión. Para poder obtener una correcta recepción, el receptor debe conocer el código, y además, estar escuchando la señal de entrada en el momento y frecuencia correctos.

Esta técnica reduce notablemente las interferencias, ya que la señal que interfiera solo afectará a la señal de datos si ambas se transmiten en la misma frecuencia simultáneamente.

Las regulaciones de la *Federal Communications Commission (FCC)* exigen que los fabricantes usen 75 frecuencias o más, por cada canal de transmisión, con un tiempo máximo en una frecuencia específica en cualquier expansión simple de 400 ms.

- **DSSS (Espectro expandido por secuencia directa)**

Esta tecnología de transmisión de radio frecuencia llamada espectro expandido por secuencia directa y más conocida como DSSS (*Direct-Sequence Spread Spectrum*), amplía el espectro mediante la expansión de frecuencia.

En esta técnica, la señal de datos en la estación emisora se combina con una secuencia de mayor ratio de bits de datos denominado *chipping code*, el cual corta los datos del usuario de acuerdo con un ratio de expansión. El *chipping code* es un patrón de *bit* redundante por cada *bit* transmitido. Esto aumenta la resistencia de la señal frente a las interferencias.

Además en caso de que se alterasen uno o más de los *bits* del patrón durante la transmisión, los datos originales se podrían recuperar gracias al incremento de la redundancia en la señal durante la transmisión.

- **OFDM (Multiplexado por división ortogonal de frecuencia)**

La tecnología de transmisión de multiplexado por división ortogonal de frecuencia, denominada OFDM (*Orthogonal Frequency Division Multiplexing*), opera cortando la señal de radio en subseñales múltiples menores que se envían en diferentes frecuencias.

Distintos estándares 802.11

La versión inicial del estándar IEEE 802.11 publicada en 1997 especificaba una velocidad de transmisión máxima de 2 Mbps.

Las transmisiones se realizaban por señales infrarrojas (IR) en la banda ISM a 2,4 GHz. Este medio de transmisión continua siendo utilizado en el resto de estándares desarrollados sobre el 802.11.

Del mismo modo, el estándar original, define como método de acceso el protocolo CSMA/CA. Este protocolo necesita una parte importante de la velocidad de transmisión para mejorar la calidad de la transmisión bajo condiciones ambientales adversas.

Hoy en día el estándar original 802.11 no se utiliza y es incompatible con los dispositivos actuales.

A continuación se exponen las evoluciones del estándar que son usados actualmente:

- **IEEE 802.11a**

Fue creado en 1999 con la intención de aumentar la velocidad máxima hasta los 54 Mbps. Esta variante opera dentro del rango de los 5 GHz para evitar las interferencias con otros dispositivos como los teléfonos inalámbricos o microondas que también operan en la frecuencia de 2,4 GHz.

Sin embargo, la nueva frecuencia presenta un alcance bastante limitado ya que las paredes y objetos bloquean esta frecuencia con mayor facilidad; además surge el inconveniente de que en muchos países esta banda está reservada a las fuerzas y organismos de seguridad.

Al operar en una frecuencia diferente es incompatible con los estándares 802.11b y g.

Utiliza tecnología OFDM soportando hasta 64 usuarios por punto de acceso.

- **IEEE 802.11b**

Al igual que el IEEE 802.11a fue creado en 1999, pero con la diferencia de seguir operando en la frecuencia 2,4 GHz. También conocido como 802.11 *High Rate* o Wi-Fi (*Wireless Fidelity*), ya que alcanza una velocidad de 11 Mbps.

El método de modulación utilizado es DSSS usando CCK (Modulación por Cambios de Código Complementarios), soportando hasta 32 usuarios por punto de acceso.

Debido a su bajo coste de implantación, este estándar es el principal responsable del gran crecimiento de las redes inalámbricas.

- **IEEE 802.11g**

Creado en 2003, se basa en la compatibilidad con los dispositivos 802.11b, ya que sigue operando en la misma frecuencia de 2,4 GHz, pero con la ventaja de ofrecer una velocidad de hasta 54 Mbps.

- **IEEE 802.11n**

Lanzado en el 2009, combina varias características de los estándares anteriores, tal es así que funciona en ambas bandas 2,4 y 5 GHz. Su principal ventaja es que puede alcanzar una velocidad máxima de hasta 540 Mbps.

Además uno de los cambios más importantes es la incorporación de la tecnología denominada Múltiple Entrada Múltiple Salida (MIMO), que consiste en el empleo de varias antenas que permiten enviar múltiples flujos de datos en paralelo, mejorando así la velocidad de transmisión de datos.

- **Comparación de variantes**

	802.11a	802.11b	802.11g	802.11n
Fecha	1999	1999	2003	2009
Velocidad Máxima	54 Mbps	11 Mbps	54 Mbps	540 Mbps
Frecuencia	5 GHz	2,4 GHz	2,4 GHz	2,4 GHz o 5 GHz
Interfaz del aire	OFDM	DSSS	OFDM/DSSS	OFDM
Alcance	30 metros	30 metros	30 metros	50 metros
Compatibilidad	Incompatible con 802.11b y 802.11g	Compatible con 802.11g. Incompatible con 802.11a	Compatible con 802.11b. Incompatible con 802.11a	Compatible con todos.

Figura 13. Comparativa estándares IEEE 802.11

Seguridad IEEE 802.11

La especificación original de 802.11 utiliza 3 mecanismos para proteger las redes inalámbricas:

- **SSID (Identificador de Servicio)**

Es una palabra compuesta por hasta 32 caracteres que identifica un punto de acceso de la red inalámbrica. Para poder acceder al punto de acceso los clientes deben conocer y tener configurado el SSID. Sin embargo, es muy sencillo conocer el SSID de un punto de acceso ya que habitualmente el mismo se distribuye por la red por medio de las señales guía (*beacon frames*).

- **Filtrado con dirección MAC**

Limita el acceso a la red a dispositivos cuya dirección MAC de su adaptador está incluida en una lista de direcciones que contiene cada punto de acceso.

- **WEP (Privacidad Equivalente a Cable)**

Es un sistema de cifrado basado en el algoritmo RC4 que protege los datos transmitidos entre los clientes y los puntos de acceso. A pesar de que el uso de WEP es opcional, la certificación Wi-Fi exige su uso con claves de 40 bits. Se recomienda el uso de alguno de los siguientes métodos para definir las claves:

- Se comparte por todas las estaciones de la red un conjunto de cuatro claves como máximo. El principal problema es que al ser distribuidas por toda la red la seguridad se ve comprometida.
- Cada cliente establece una relación de claves con otra estación. Este método es más seguro, ya que menos estaciones tienen las claves de la red, sin embargo existe el problema de su distribución en redes con gran número de estaciones.

Tras la implantación del estándar inicial en los ámbitos profesional y personal, se fueron detectando vulnerabilidades y fallos de seguridad que se han ido corrigiendo y reforzando con otros estándares y protocolos que vemos a continuación:

- **802.1X**

Para dar solución a los fallos de seguridad de WEP, el IEEE creó el estándar 802.1X. En él, se implementa un mecanismo de seguridad que proporciona control de acceso entre los dispositivos inalámbricos clientes, los puntos de acceso y los servidores.

Se utilizan llaves dinámicas en lugar de las estáticas de la autenticación WEP. Además, se hace necesario un protocolo de autenticación para permitir el reconocimiento mutuo. Por lo que se hace necesario un servidor que proporcione dicho servicio de autenticación remota a los nuevos usuarios (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).

- **WPA (Wi-Fi Protected Access)**

Se creó como medida temporal en sustitución de la seguridad WEP mientras se trabajaba en finalizar el estándar IEEE 802.11i. Se aportan mejoras sustanciales en la seguridad en diferentes aspectos, como son autenticación, cifrado e integridad de la información.

- **Autenticación:** Ha sido diseñado para utilizar el protocolo 802.1X, realizando autenticación mediante un servidor dedicado a ello. Este método se denomina WPA-Enterprise.

Sin embargo, para reducir costes, y previendo su uso a nivel no profesional, permite prescindir de él mediante el uso de una clave precompartida. Este tipo de autenticación se denomina comúnmente WPA-Personal.

- **Cifrado:** Se sigue utilizando el mismo cifrado que WEP, el algoritmo RC4, sin embargo se introducen unas modificaciones con el fin de fortalecerlo, como son una clave de 128 bits (en lugar de 40) y un vector de inicialización de 48 bits. Además se implementa el Protocolo de Integridad de Clave Temporal (TKIP), el cual modifica las claves dinámicamente a medida que se van utilizando.
- **Integridad:** Se implementa un código de integridad del mensaje (MIC), más conocido como *Michael*. Además, se incluye un contador de tramas con el fin de protegerse contra ataques de repetición.
- **WPA2 (Wi-Fi Protected Access 2)**

Se basa en el estándar 802.11i una vez que este fue ratificado en 2004. Su principal novedad respecto a WPA es que cambia el algoritmo de cifrado a AES (*Advanced Encryption Standard*).

2.5 WMAN (Redes inalámbricas de área metropolitana)

Las redes inalámbricas de área metropolitana, denominadas WMAN por sus siglas en inglés *Wireless Metropolitan Area Network*, permiten establecer conexiones inalámbricas en un área de hasta 50 km, cubriendo así toda una ciudad o incluso conectando varias ciudades cercanas sin necesidad de cablear.

En este tipo de redes se encuentran tecnologías basadas en el estándar IEEE 802.16, más conocido popularmente como WiMax (*Worldwide Interoperability for Microwave Access*). Aunque también existen otras tecnologías como LMDS (*Local Multipoint Distribution Service*).

2.5.1 WiMax

WiMax son las siglas de *Worldwide Interoperability Microwave Access*, o en español Interoperabilidad Mundial para el Acceso por Microondas. Surge en 2002, como la denominación comercial que el grupo *WiMax Forum* le da a dispositivos que cumplen el estándar IEEE 802.16.

Fue creado con el objetivo de proporcionar acceso a Internet de alta velocidad en un rango de cobertura de varios kilómetros (hasta 48 kilómetros y velocidades de hasta 70 Mbps).



Figura 14. Logotipo WiMax

Su principal ventaja es que no necesita que exista visibilidad directa entre el emisor y el receptor. Esta tecnología denominada NLOS (*Non Line of Sight*) es capaz de atravesar los obstáculos pequeños, sin embargo, si como es lógico, si existen muchos obstáculos entre el emisor y receptor el rendimiento se resiente considerablemente.

Las revisiones del estándar IEEE 802.16 se dividen en dos categorías¹¹:

- **WiMAX fijo o IEEE 802.16-2004**

Se denomina fijo porque el receptor utiliza una antena fija situada en algún lugar estratégico, es algo similar a una antena de televisión por satélite.

¹¹ WiMax - 802.16 - Interoperabilidad mundial para acceso por micro
<http://es.kioskea.net/contents/wimax/wimax-intro.php3>

Puede funcionar en las bandas de frecuencia 2.5 GHz y 3.5 GHz, para las que se necesita una licencia específica, pero también en la banda 5.8 GHz que está exento de licencia.

- **WiMAX móvil o IEEE 802.16e**

A finales del 2005, surge este estándar que aplica una modificación sobre la especificación inicial 802.16-2004, permitiendo utilizarse en terminales móviles. Aunque esta ventaja trae asociada una disminución del rango y la velocidad máxima.

- **Comparación de variantes**

	<i>IEEE 802.16-2004</i>	<i>IEEE 802.16e</i>
<i>Fecha</i>	2004	2005
<i>Velocidad Máxima</i>	75 Mbps	30 Mbps
<i>Frecuencia</i>	2-11 GHz (3.5 GHz Europa)	2-6 GHz
<i>Alcance</i>	10 km	3,5 km

Figura 15. Comparativa estándares WiMax

2.5.2 LMDS

El Sistema de Distribución Local Multipunto o *LMDS* (*Local Multipoint Distribution Service*) es una tecnología de conexión de radio inalámbrica con un gran ancho de banda, permitiendo servicios de internet de alta velocidad, voz y multimedia.

La transmisión se denomina multipunto porque se realiza desde un único punto, la estación base, hacia distintas instalaciones receptoras. Mientras que la comunicación inversa se realiza punto a punto.

Utiliza señales de alta frecuencia, las cuales no pueden atravesar obstáculos, por lo que entre el emisor y el receptor debe estar libre de ellos o no habrá servicio. Además se resienten en condiciones meteorológicas adversas como niebla o lluvia.

También hay que considerar que las distancias de transmisión son cortas, hasta un máximo de 35 km.

2.6 WWAN (Redes inalámbricas de área extensa)

Las redes inalámbricas de área extensa, denominadas WWAN por sus siglas en inglés *Wireless Wide Area Network*, son las redes inalámbricas con mayor alcance. Por ello, los teléfonos móviles utilizan esta clase de redes.

Dentro de estas redes podemos encontrar las siguientes tecnologías:

- **GSM (*Global System for Mobile Communication*):** Es un sistema estándar para comunicación mediante teléfonos móviles que incorpora tecnología digital, permitiendo así envío y recepción de datos. A los móviles que usan esta tecnología se les conoce por móviles 2G.
- **GPRS (*General Packet Radio Service*):** Es una optimización de GSM que permite la transmisión de datos mediante conmutación de paquetes. Alcanza velocidades de datos de hasta 115 Kbps. Comúnmente se conoce como 2.5G.
- **UMTS (*Universal Mobile Telecommunication System*):** También conocida como WCDMA (*Wideband Code Division Multiple Access*). Es la tecnología usada por los móviles de tercera generación (3G). Provee de banda ancha en la telefonía móvil, por lo que añade capacidades multimedia como reproducción en línea de audio y video, videollamadas y juegos en red.
- **LTE (*Long Term Evolution*):** Es un nuevo estándar de la norma 3GPP. Algunos lo consideran la evolución natural de la norma 3GPP UMTS (3G), pero otros consideran que es un nuevo concepto de arquitectura. Sus principales ventajas son el aumento de la eficiencia, y por lo tanto de la velocidad de transmisión, y la reducción de los costes. Es lo que habitualmente se conoce como 4G.

Capítulo 3

Redes WLAN

En este capítulo se profundiza en las redes de tipo WLAN, con el fin proporcionar al lector de la información necesaria para entender las características detalladas y los problemas de seguridad que se plantean en ellas.

El mundo de las telecomunicaciones en los últimos años ha cambiado radicalmente su filosofía adaptándola a las necesidades de movilidad que han ido surgiendo.

Hoy en día es fundamental tener acceso a información en cualquier momento y en cualquier lugar. Por ejemplo, si un trabajador tiene acceso a la información sin necesidad de desplazarse a un punto concreto o de permanecer inmóvil en su puesto de trabajo, podrá aumentar la productividad y competitividad de la empresa.

Desde hace más de 20 años se han estado utilizando en entornos industriales, centros de investigación, y oficinas empresariales. Pero ha sido en los últimos años, cuando los avances en la tecnología lo han permitido, ha llegado masivamente a todos los entornos, incluido el ámbito doméstico, reemplazando así a las tradicionales redes cableadas.

Algunos de los puntos clave para esta rápida expansión son los siguientes:

- **Aparición de estándares y normalización de la tecnología.** La ausencia de estos, provocaba que cada fabricante utilizara su propia tecnología, con sus frecuencias y parámetros particulares. Lo que desembocaba en que soluciones de distintos fabricantes fueran totalmente incompatibles entre sí.
- **Reducción de costes.**
- **Aumento de las prestaciones.** El aumento del alcance y sobre todo la velocidad de transmisión hacen que las redes inalámbricas, aunque aún distantes del rendimiento de una red cableada, cumplan con las necesidades para la gran mayoría de los casos de uso habituales.
- **Generalización de dispositivos portátiles.** La llegada al público en general de los *smartphones* y ordenadores cada vez más fáciles de movilizar, crean la necesidad de estar conectado en todo momento, ya

sea en el lugar de trabajo, en el hogar, en un centro comercial o cualquier otro lugar.

- **Facilidad de instalación.** Su principal ventaja respecto a las redes tradicionales, es su facilidad de instalación, ya que deja de ser necesario realizar un cableado de las instalaciones.

A pesar de que todo parecen ventajas, aún hoy día, este tipo de redes, están lejos del rendimiento de una red cableada, lo que en muchas ocasiones conlleva en lugar de ser reemplazadas, a que se complementen entre sí.

3.1 Antecedentes

El origen de su nacimiento puede ser considerado con la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica.¹²

Tras el éxito de este experimento, continuaron las investigaciones con infrarrojos, y además se ampliaron a las microondas utilizando el esquema del espectro extendido (*spread spectrum*).

Tras varios años de estudios, en mayo de 1985, la Agencia Federal del Gobierno de EEUU (FCC *Federal Communications Commission*) encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (*Industrial, Scientific and Medical*) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en espectro extendido.

Esta asignación fue un punto de inflexión, ya que se consideró como un respaldo importante para esta tecnología, multiplicando el interés de los diferentes fabricantes en concretarla más allá de experimentos de laboratorio.

En los siguientes años se continuó trabajando, hasta que por fin, en mayo de 1991 se publicaron diferentes ensayos prácticos de redes inalámbricas que por primera vez alcanzaban e incluso superaban la velocidad mínima establecida por el IEEE 802, de 1 Mbps. Consiguiendo así, las primeras redes que se ajustaban a la definición del estándar.

12 Redes de área local: administración de sistemas informáticos

Escrito por Antonio Blanco Solsona, José Manuel Huidobro Moya, J. Jordán Calero

3.2 Normalización

En 1990, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las redes inalámbricas. Pero no es hasta 1994 cuando aparece el primer borrador, y en junio de 1997 que se da por finalizada la norma.

En 1992 se crea Winforum, consorcio liderado por Apple y formado por empresas del sector de las telecomunicaciones y de la informática para conseguir bandas de frecuencia para los sistemas PCS (*Personal Communications Systems*). En ese mismo año, el ETSI (*European Telecommunications Standards Institute*), a través del comité ETSI-RES 10, inicia actuaciones para crear una norma a la que denomina HiperLAN (*High Performance LAN*) para, en 1993, asignar las bandas de 5,2 y 17,1 GHz.

En 1993 también se constituye la IRDA (*Infrared Data Association*) para promover el desarrollo de las redes inalámbricas basadas en enlaces por infrarrojos.

En 1996, finalmente, un grupo de empresas del sector de informática móvil y de servicios forman el *Wireless LAN Interoperability Forum* (WLI Forum) para potenciar este mercado mediante la creación de un amplio abanico de productos y servicios interoperativos. Entre los miembros fundadores de WLI Forum se encuentran empresas como ALPS Electronic, AMP, Data General, Contron, Seiko, Epson y Zenith Data Systems.

3.3 Ventajas

Como hemos venido comentando, las redes inalámbricas ofrecen una serie de ventajas e inconvenientes respecto a la red cableada tradicional. A continuación vamos a enumerar sus principales ventajas:

- **Simplicidad en la instalación:** La instalación básica consiste en conectar el punto de acceso en la entrada de la red. Los dispositivos cliente normalmente no requieren instalación, ya que hoy día la gran mayoría tienen el hardware incorporado de fábrica.

Se elimina la necesidad de cableado en las instalaciones.

- **Movilidad:** Permite acceder a la red y por tanto a la información desde cualquier lugar dentro del entorno donde está desplegada la red inalámbrica. Este punto es muy importante, ya que en ciertos entornos empresariales, el acceso a la información en tiempo real implica una mayor productividad.
- **Reducción de costos:** Al no requerir cableado, se reduce considerablemente el costo de la misma, no solo en materiales, sino también en las obras necesarias para realizar dicho cableado, así como en el mantenimiento del mismo.
- **Escalabilidad:** Dada la versatilidad de topologías, permite que estas redes sean escalables según las necesidades de cada momento, tanto en cobertura como en número de usuarios soportados. Tan solo sería necesario incorporar más hardware a la red para cubrir así los nuevos requerimientos.

3.4 Inconvenientes

Pero no todo son ventajas en este tipo de redes, también existen una serie de inconvenientes:

- **Alcance limitado:** El rango de alcance de un punto de acceso es bastante limitado y queda restringido a un área determinada, habitualmente pueden cubrir entre 20 y 200 metros dependiendo de varios factores como son la potencia del punto de acceso y del dispositivo cliente, los obstáculos en las instalaciones y posibles interferencias.

Este inconveniente puede derivar en problemas de conectividad en los lugares más alejados del punto de acceso. Sin embargo, es salvable utilizando amplificadores de señal o repetidores.

- **Velocidad de transmisión:** La velocidad máxima de transmisión, dependiendo de la variación del estándar a utilizar, varía entre 54 Mbps y 300 Mbps, aunque la velocidad real es mucho menor ya disminuye sensiblemente por la distancia al punto de acceso.

Aun así son velocidades mucho más que suficientes para cubrir el uso en hogares y en gran parte de los entornos empresariales. Sin embargo, están a mucha distancia de las velocidades reales que se consiguen en redes cableadas (1 Gbps).

- **Seguridad:** Es uno de sus principales inconvenientes. El problema no viene tanto por sus debilidades de diseño, sino por la falta de conocimiento y administración de las mismas.

A pesar de que, como veremos, los mecanismos de seguridad implementados en los diferentes estándares tienen sus debilidades, la gran mayoría de los casos en los que se produce una violación de la seguridad de este tipo de redes, viene dada por un mal uso de esos mecanismos, o incluso por la ausencia de ellos.

3.5 Elementos Hardware

A continuación vamos a ver los principales elementos hardware que son empleados para la implantación de una de infraestructura que de soporte a una red inalámbrica.

A pesar de que los vamos a clasificar de una manera formal, en la realidad los equipos de los fabricantes suelen integrar modos híbridos de funcionamiento. Por ejemplo es muy normal encontrar *routers* que operan además como puntos de acceso, puentes o repetidores.

- **Puentes (*Bridges*)**

Son utilizados para conectar dos o más redes locales fijas. La conexión se realiza en la capa de enlace, el nivel 2 del modelo OSI.

Se utiliza en redes que están separadas por una distancia que, o bien económicamente o logísticamente, se hace más eficiente unirlos de manera inalámbrica.

Cada red cableada se conecta físicamente al puente, y este a su vez se comunica de manera inalámbrica con su homólogo en la otra red. Para poder establecer la comunicación, ambos puentes deben compartir los parámetros de configuración.

Además no existe ninguna limitación en el número de puentes que se pueden enlazar, lo que puede resultar para unir redes muy distantes o con muchos obstáculos.

- **Enrutadores (*Routers*)**

Son elementos que tienen capacidad para encaminar los paquetes que circulan a través de ellos, esto es utilizar los niveles 3 y 4 del modelo OSI.

Adicionalmente poseen funcionalidades de red avanzadas, como son traducción de direcciones por NAT, servidor DHCP de direccionamiento propio, implementación de mecanismos de seguridad como *firewall*, listas de acceso por dirección MAC, control parental y restricción de uso por diferentes factores entre otros. Incluso los modelos más avanzados introducen gestión de redes privadas virtuales (VPNs).

- **Tarjetas de red inalámbricas (TR)**

Las tarjetas de red inalámbricas son el punto de conexión de los equipos a la red. Mediante ellas reciben y envían la información sobre la red.

Habitualmente vienen integradas en los dispositivos, ya sean *smartphones*, ordenadores portátiles o de sobremesa. Aunque también existen en el mercado dispositivos que se pueden conectar mediante PCMCIA/PCI o USB en caso de que el equipo no lo tenga integrado.

También se les conoce por sus siglas en inglés NIC (*Network Interface Card*).

- **Punto de Acceso (AP – Access Point)**

El punto de acceso recibe los paquetes de las tarjetas de red de las que conste para su centralización o para su encaminamiento.

Permite la comunicación a nivel 2 del modelo OSI.

- **Repetidores (*Repeaters*)**

Se utilizan para ampliar la cobertura de los puntos de acceso mediante la regeneración y reenvío de información.

Poseen un único interfaz inalámbrico, mediante el cual se conectan tanto al punto de acceso del que repiten la señal, como también dan servicio a los equipos inalámbricos que se le subscriben.

La configuración debe ser la misma que la del punto de acceso al que se conecta.

La principal desventaja es que disminuye hasta en un 50% su eficiencia, ya que toda la información que recibe desde los equipos debe ser retransmitida al punto de acceso.

Aunque en teoría se pueden encadenar varios repetidores para ampliar el alcance de la red, en la práctica no es recomendable, ya que surgen innumerables problemas de retardo y colisiones, resultando una experiencia de usuario muy pobre para los equipos conectados a los repetidores más lejanos.

3.6 Arquitecturas o topologías de red WLAN

La inmensa mayoría de redes inalámbricas que existen actualmente, ya sea en el ámbito empresarial o doméstico, utilizan una topología en modo infraestructura con uno o más puntos de acceso.

Aunque menos habitual, es posible una arquitectura alternativa denominada modo Ad-Hoc, esta puede darse en entornos de red cerrados, sin conexiones fuera de ella, donde prima un intercambio eficiente de información entre todos los equipos que componen la red.

Existen tres topologías de red WLAN:

- **Grupo de servicio básico (BSS, *Basic Service Set*):** Topología de red formada por un punto de acceso y estaciones inalámbricas.
- **Grupo de servicio extendido (ESS, *Extended Service Set*):** Cuando existe más de una BSS interconectadas entre ellas.
- **Grupo de servicio independiente (IBSS, *Independent Basic Service Set*):** Cuando una BSS está formada únicamente por estaciones inalámbricas, operando por lo tanto en modo ad-hoc.

A continuación se detallan las principales características de estas arquitecturas:

3.6.1 Modo IBSS

El modo IBSS, o más conocido como ad-hoc, es aquel en el cual las estaciones inalámbricas se comunican directamente entre sí, sin la necesidad de un punto de acceso.

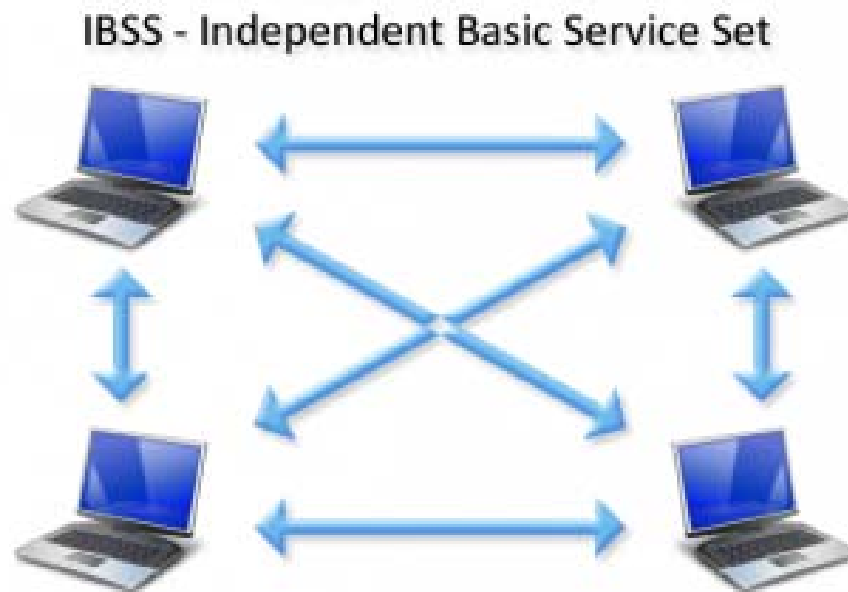


Figura 16. Topologías de red WLAN. IBSS

3.6.2 Modo BSS

El modo BSS, también conocido como infraestructura, utiliza un punto de acceso para realizar la comunicación de las estaciones inalámbricas. Este punto de acceso realiza las funciones de coordinación. Todo el tráfico desde y hacia las estaciones inalámbricas tiene que atravesar el punto de acceso, por lo que hay una evidente pérdida de eficiencia cuando dos estaciones de la misma red desean comunicarse entre sí (la información es enviada desde el origen al punto de acceso, y del punto de acceso al destino final).

La utilización de esta arquitectura resulta apropiada cuando la mayor parte del tráfico tiene como origen o destino una red exterior a la cual está conectada el punto de acceso. Este modo es el que se emplea normalmente para conectar una red inalámbrica con Internet a través del acceso del router/modem.

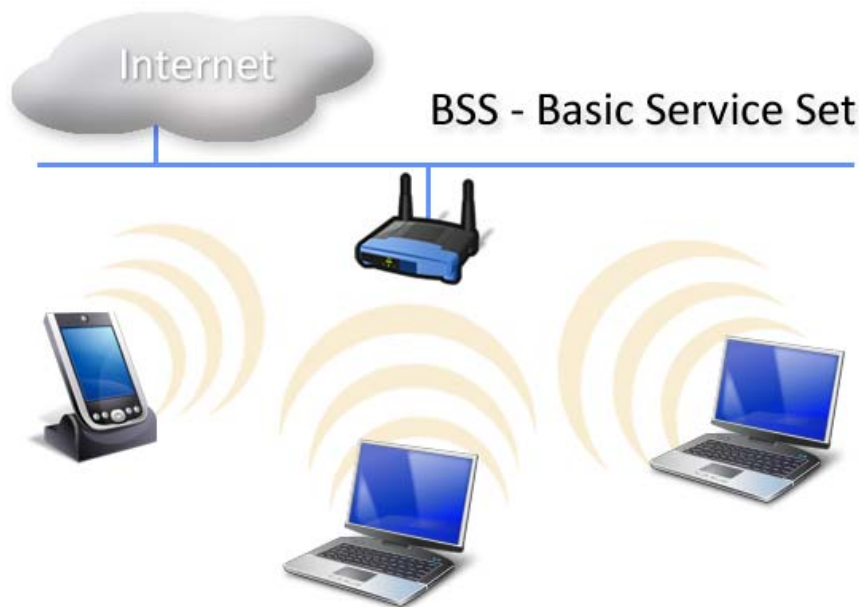


Figura 17. Topologías de red WLAN: BSS o infraestructura

3.6.3 Modo ESS

El modo ESS está compuesto por una serie de redes BSS que mediante un mecanismo de comunicación entre los puntos de acceso de dichas redes, denominado sistema de distribución, forman una única subred.

Este modo es habitualmente utilizado en redes WLAN de empresas con más de un punto de acceso.

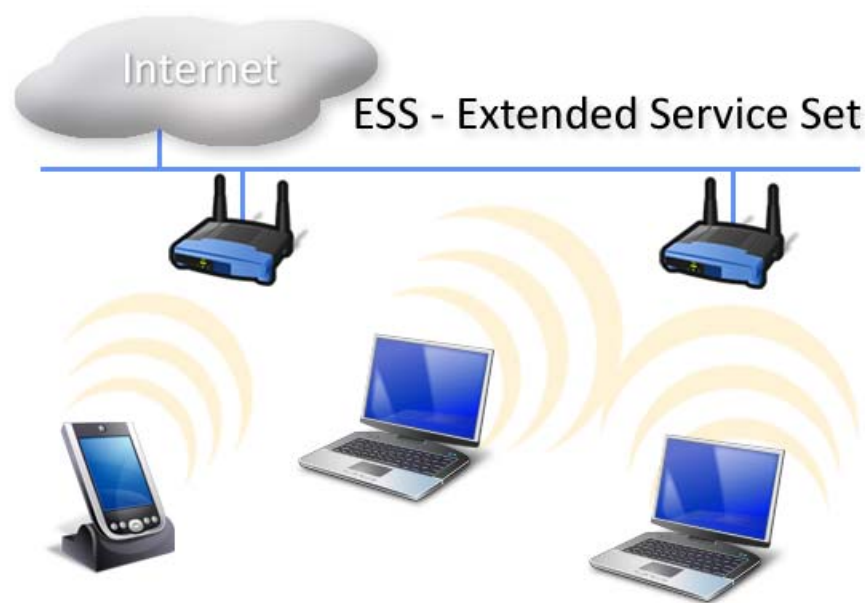


Figura 18. Topologías de red WLAN: ESS

Existen diferentes sistemas de distribución, que en general se podrían clasificar según el medio físico que utilizan:

- **Sistemas de distribución cableados:** Los puntos de acceso se relacionan mediante Ethernet, ya sea directamente o a través de una red cableada.
- **Sistemas de distribución inalámbricos:** Se relacionan a través de un enlace inalámbrico con rutas preconfiguradas y estáticas.

3.6.4 Modos de actuación

Además de la topología de las redes inalámbricas comentadas anteriormente, es interesante conocer que a su vez, cada estación de la red puede tener diferentes modos de funcionamiento que se describen a continuación:

- **Modo Máster:** La estación actúa como punto de acceso siendo capaz de dar servicio y, a la vez, gestionar las conexiones de otros dispositivos.
- **Modo monitor:** Este modo permite a la estación capturar paquetes de la red sin llegar a asociarse a ella, es decir, permite monitorizar la red sin transmitir tráfico a la misma.
- **Modo promiscuo:** Es similar al modo monitor, pero en este caso es necesario que la estación esté asociada a la red.

Estos dos últimos modos de captura de paquetes, son habitualmente utilizados para realizar ataques a redes WLAN.

Capítulo 4

Ataques a redes WLAN

Este capítulo se detalla las principales debilidades y agujeros de seguridad que tienen las redes WLAN. Concienciando así al lector de la necesidad de tomar medidas al respecto.

Para poder asegurar adecuadamente una red inalámbrica, es necesario conocer cuáles son sus amenazas potenciales.

Existen diversos métodos para descubrir, interceptar y atacar una red inalámbrica.

Estas amenazas se pueden englobar en dos grandes grupos:

- **Ataques Pasivos:** Este tipo de ataques tienen como principal objetivo obtener información de la red o de los equipos que la componen. Se considera como el primer paso para un ataque posterior. En este grupo estarían actividades tales como monitorización y escuchas de la red.
- **Ataques Activos:** Son ataques intrusivos que habitualmente suponen una modificación del flujo de datos o la introducción de falsos flujos en la transmisión de los mismos. Sus principales objetivos son realizar una suplantación de identidad con el fin de obtener información o bien colapsar los servicios de la red.

4.1 Ataques pasivos

4.1.1 Espionaje (Surveillance)

Consiste en observar el entorno para recopilar información relacionada con la arquitectura de la red. No requiere ningún tipo de equipo especial, tan sólo es necesario tener acceso físico a la instalación.

A pesar de que a priori puede parecer poco útil, un atacante puede obtener mucha información de utilidad a utilizar en un ataque posterior. Por ejemplo la localización de los puntos de acceso y antenas.

4.1.2 Escuchas (Sniffing)

Consiste en monitorizar la red para capturar información que transita en ella, como pueden ser direcciones MAC de los equipos conectados, IPs, usuarios, contraseñas y clave WEP entre otras.

Para poder llevar a cabo este tipo de monitorización se debe disponer de una tarjeta inalámbrica actuando en modo promiscuo o monitor para poder escuchar el tráfico que circula por la red. Dada la enorme cantidad de tráfico que se genera en una red, para poder organizar y hacer legible esa información se hace necesario utilizar un software específico que se denomina *sniffer*. Algunos de los más utilizados son el AirSnort para Linux y el NetSlumber para Windows.

4.1.3 Wardriving

Es un caso particular del ataque de escuchas, donde el atacante, equipado con un dispositivo móvil, software de rastreo y un GPS, simplemente pasea tratando de localizar puntos de acceso inalámbricos. En el momento en que detecta la existencia de la red, se realiza un análisis de la misma.

4.1.4 Warchalking

Es un lenguaje de símbolos que se utiliza para marcar sobre el lugar de la existencia de una red inalámbrica.

Cada símbolo contiene la siguiente información:

- SSID, es decir, el nombre del punto de acceso.
- Si la red es abierta (sin clave de acceso) o cerrada (con clave de acceso). Y en dado caso, el tipo de cifrado.
- Por último se indica la velocidad de la red.

Con estos datos, cualquier persona, podrá utilizar la red haciendo uso de la información ofrecida por los símbolos.




KEY	SYMBOL
NODO ABIERTO	ssid  bandwidth
NODO CERRADO	ssid 
NODO WEP	ssid access contact  bandwidth

Figura 19. Lenguaje WarChalking

4.1.5 Descubrimiento de contraseña

Este tipo de ataques se realizan con el fin de descubrir la contraseña que un usuario utiliza para conectar a la red. Para poder llevar a cabo este ataque es necesario escuchar y recopilar el tráfico durante cierto tiempo, una vez que disponemos de suficiente información podemos realizar cualquiera de los siguientes métodos:

- **Ataques por fuerza bruta:** Son aquellos que intentan descubrir la clave de cifrado mediante la prueba de todas las combinaciones posibles.

Este método, por definición, siempre logra su objetivo, el principal limitante que tiene es la necesidad de recursos y tiempo. Ante contraseñas suficientemente largas y complejas, el número de ataques a realizar se dispara de manera exponencial, por lo que resulta muy difícil de lograr.

- **Ataques por diccionario:** Son similares a los ataques por fuerza bruta, la única diferencia es que no se prueban todas las posibles combinaciones, sino que se utiliza una lista de palabras probables, generalmente tomadas de un glosario de nombres y palabras. Si la clave utilizada está en el diccionario se reduce drásticamente el tiempo y los recursos necesarios para descubrirla.

4.1.6 Descubrimiento de ESSID ocultos

El proceso de conexión de un usuario a una red inalámbrica consiste en la autenticación y asociación a un punto de acceso. Para ello, es necesario que el usuario conozca previamente la existencia de la red.

El SSID (*Service Set Identifier*) es un código que se incluye en todos los paquetes que se transmiten en una red inalámbrica para poder identificarlos

como tráfico de la red, por lo tanto todos los dispositivos que se comuniquen entre sí dentro de la misma red deben conocer el mismo SSID.

En redes inalámbricas funcionando en modo ad-hoc el SSID se denomina BSSID (*Basic Service Set Identifier*) y normalmente se usa la dirección MAC del punto de acceso. Por el contrario, para redes en modo infraestructura, el SSID es conocido como ESSID (*Extended Service Set Identifier*) y consiste, habitualmente, en un máximo de 32 caracteres alfanuméricos que componen el nombre de la red.

Para descubrir dicho ESSID existen dos posibles métodos:

- **Escaneo Pasivo:** El dispositivo del usuario espera recibir alguna señal del punto de acceso. Habitualmente los puntos de acceso emiten *Beacon Frames* cada cierto tiempo, estas tramas suelen contener el ESSID. Una vez descubierto el ESSID se puede iniciar el proceso de conexión y asociación al punto de acceso.

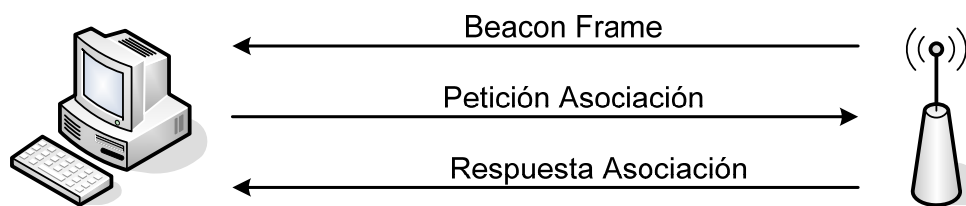


Figura 20. Escaneo Pasivo

- **Escaneo Activo:** El usuario realiza peticiones a un punto de acceso y espera la respuesta. También se puede enviar una trama de petición conocida como *Probe Request* con un ESSID determinado para ver si algún punto de acceso responde a dicha petición.

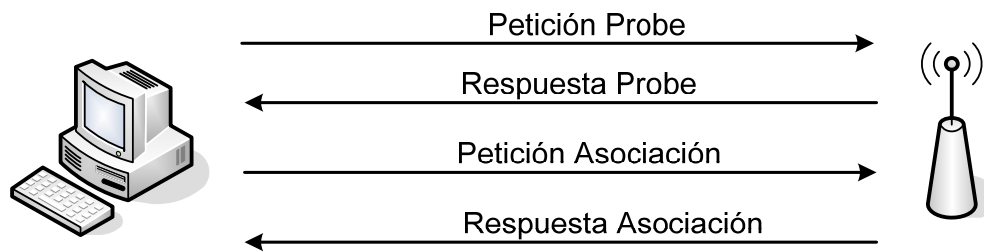


Figura 21. Escaneo Activo

No emitir *Beacon Frames* o emitirlo sin el ESSID permite que solo puedan conectar a la red los usuarios que conozcan el ESSID de antemano. Este tipo de redes se denominan cerradas.

Sin embargo, el usuario puede descubrir el ESSID de la red si escucha y captura tramas de petición de *Probe* enviadas por otros usuarios de la red. El envío de estas tramas se puede forzar realizando un ataque de denegación de servicio mediante el cual se consigue desasociar un usuario de la red, provocando que este vuelva a realizar el proceso de asociación a la misma.

4.2 Ataques activos

A continuación se detallan los principales ataques activos en redes WLAN.

4.2.1 Punto de acceso no autorizados/Rogue APs

Se denomina Rogue AP a los puntos de acceso que se conectan a una red sin autorización, por lo tanto, con casi toda seguridad no se ajustan a la política de seguridad de la red ya que no son gestionados por los administradores de la misma.

Esto permite que cualquier dispositivo pueda conectar a la red a través de este punto de acceso no autorizado, vulnerando así todos los mecanismos basados en el cifrado de la información. Por lo tanto, se abre una puerta a todo tipo de ataques a la red.

Para poder instalar un *Rogue AP* es necesario tener acceso físico a la instalación de la red.

Para detectar estos puntos de acceso no autorizados existen diversas herramientas, muchas de ellas permiten, además, deshabilitar los puntos de acceso no autorizados que hayan sido detectados. El funcionamiento de dichas herramientas se basa en el escaneo por parte de un punto de acceso, el cual envía la información a un sistema centralizado que analiza y decide si el punto de acceso detectado es autorizado o no.

Algunas de las herramientas que ofrecen la funcionalidad anteriormente comentada más conocidas del mercado son Airdefense, Airmagnet o Airwave.

4.2.2 Spoofing

Consiste en suplantar parámetros de la red que permanecen invariables durante las diferentes fases de autenticación, conexión, etc.

Con este tipo de ataque el atacante puede suplantar la identidad de un usuario de la red.

Para obtener la información necesaria para realizar la suplantación debe existir una fase previa en la cual se emplee algún tipo de ataque pasivo.

Los principales tipos de *spoofing* utilizados en redes inalámbricas son los siguientes:

- **IP Spoofing:** Consiste en realizar una suplantación de IP. Se hace mediante la modificación de los paquetes TCP/IP reemplazando la dirección IP origen por la que se desea suplantar.

En esta técnica se consigue suplantar la identidad para el envío de paquetes en la red. Sin embargo, los paquetes de respuesta serán recibidos por el equipo que tenga la dirección IP real. Este equipo, al detectar respuestas de envíos no realizados, podría implementar medidas como cortar la conexión.

- **Mac Spoofing:** Consiste en la modificación de la dirección MAC del dispositivo con el fin de que los paquetes que envíe sean identificados como enviados por otro dispositivo diferente.

Se suele utilizar para engañar a los sistemas que tienen configurada seguridad por filtrado MAC.

- **ARP Spoofing:** Es la suplantación de identidad mediante la modificación de la tabla ARP (*Address Resolution Protocol*) del servidor que se desea atacar.

El protocolo Ethernet, a diferencia de lo que se cree habitualmente, no trabaja mediante direcciones IP directamente, sino que utiliza las direcciones MAC para identificar el origen o destino de cada paquete de red.

Cuando un equipo desea enviar un paquete a una IP determinada, consulta su tabla ARP local para determinar a qué MAC corresponde. Si es la primera vez o ha expirado, la tabla no contendrá esa información, por lo que sigue los siguientes pasos:

1. El equipo que desea comunicarse enviará una trama *ARP-Request* dirigida a todos los equipos de la red (*broadcast*).
2. El equipo con la IP requerida responde con una trama *ARP-Reply* indicando la dirección MAC que posee.
3. Al recibir la respuesta con la dirección MAC, guarda una entrada en su tabla ARP local con la relación IP-MAC para ser utilizada en los sucesivos envíos de paquetes.

Para conseguir falsear la tabla ARP de un servidor, el atacante envía una serie de tramas de solicitud y respuesta ARP modificadas.

De esta forma, consigue que utilice información falsa y envíe los paquetes al equipo atacante en vez de hacerlo al destino original.

Dado que el protocolo ARP trabaja a nivel 2 del modelo OSI (enlace de datos), esta técnica solo puede ser utilizada dentro de redes locales.

- **DNS Spoofing:** Suplantación de identidad por nombre de dominio. El ataque consiste en falsear la información de un servidor DNS, para que ante una consulta, la relación dominio-IP se resuelva con información falsa.

Por funcionamiento del protocolo DNS, al falsear un servidor, es posible que se propague esa información falsa a la caché DNS de otros servidores, a esto se le denomina envenenamiento (DNS *Poisoning*).

Basándose en el *spoofing* se pueden realizar otros ataques como:

- Man in the middle
- Secuestro de sesiones
- Denegación de servicio

4.2.3 Man in the middle

Este ataque está basado en el *spoofing* y consiste en interponerse entre dos elementos de la red. De este modo el atacante intercepta y modifica los datos para suplantar la identidad de los sistemas implicados en la comunicación interceptada.

4.2.4 Secuestro de sesiones (*Hijacking*)

Es un término muy amplio, en general, se denomina secuestro de sesiones a toda acción mediante la cual el atacante consigue adueñarse de conexiones de red, sesiones de terminal, servicios y puntos de acceso entre otros.

4.2.5 Denegación de servicio (DOS)/Jamming

El objetivo no es acceder a la red ni conseguir información de la misma, sino inutilizarla para que otros usuarios no puedan acceder a ella durante un período indefinido de tiempo. Lo más habitual es que este tipo de ataques vaya dirigido contra servidores de compañías de acceso público, impidiendo el desempeño normal de sus actividades, con el fin de dañar la reputación de la compañía.

Generalmente, estos ataques se dividen en dos clases:

- **Las denegaciones de servicio por saturación:** Saturan el servidor con tal número de solicitudes para conseguir que no pueda responder a las solicitudes reales.
- **Las denegaciones de servicio por explotación de vulnerabilidades:** Aprovechan alguna vulnerabilidad existente en el sistema para atacarlo y volverlo inestable.

Para que este tipo de ataque sea más eficaz, lo habitual es realizarlo desde varios equipos diferentes, este caso se conoce como sistema distribuido de denegación de servicio (DDOS, *Distributed Denial of Service*).

Capítulo 5

Mecanismos de seguridad en redes WLAN

Como hemos visto anteriormente existen distintos tipos de redes inalámbricas, como objeto de este trabajo nos centraremos en las más utilizadas tanto en el ámbito empresarial como en el personal, las redes WLAN.

En la actualidad, el estándar 802.11 está implantado en la gran mayoría de entornos empresariales, docentes y domésticos. Este sistema de comunicación lleva consigo una serie de ventajas respecto a las redes cableadas, pero al mismo tiempo introducen nuevos peligros y amenazas si, por desconocimiento, no se configuran correctamente, o por inacción, se dejan los valores predeterminados por cada fabricante.

5.1 Mecanismos de seguridad para impedir acceso a la red

5.1.1 Autenticación

Cuando un cliente desea encontrar y conectar a una red inalámbrica debe seguir el siguiente proceso:

1. Para detectar e identificar los puntos de acceso disponibles, el cliente escucha las señales de gestión (*beacon frames*) que transmiten los puntos de acceso en periodos de tiempo regulares.

En caso de que el cliente conozca el ESSID del punto de acceso al que desea conectarse, puede enviar una trama *probe request* con el ESSID y esperar la respuesta del punto de acceso.

2. Teniendo identificado el punto de acceso al que se quiere conectar, el cliente y el punto de acceso intercambian información, mediante lo que se denomina *management frames*, con el fin de autenticarse mutuamente. Existen diferentes mecanismos de autenticación que se detallarán más adelante.
3. Una vez autenticado con éxito, el cliente debe asociarse al punto de acceso, para ello envía una trama *association request*, la cual debe ser respondida con una trama de confirmación denominada *association response*.
4. Establecida la autenticación y asociación, el cliente se convierte en un dispositivo más de la red inalámbrica, pudiendo así iniciar el intercambio de datos en la red.

El siguiente diagrama muestra los pasos anteriormente descritos:

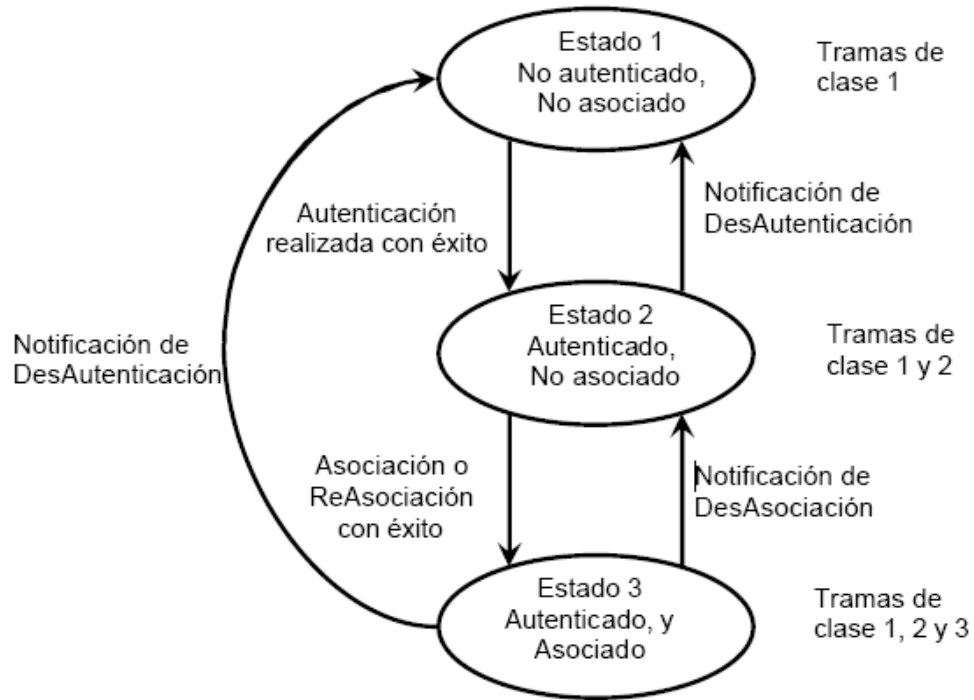


Figura 22. Mecanismo de autenticación

Como comentábamos anteriormente, existen distintos sistemas de autenticación, los vemos a continuación:

OSA: Sistema de autenticación abierta (*Open System Authentication*)

Es el mecanismo de autenticación por defecto para las redes 802.11. No se requiere autenticación, por lo que, una vez el cliente ha negociado los parámetros de red, ya se considera autenticado.

Al no existir autenticación, cualquier cliente que desee conectarse a la red lo podrá hacer.

Con este sistema, todas las tramas de gestión en la comunicación entre el punto de acceso y cliente, y viceversa, son enviadas sin ningún tipo de cifrado.

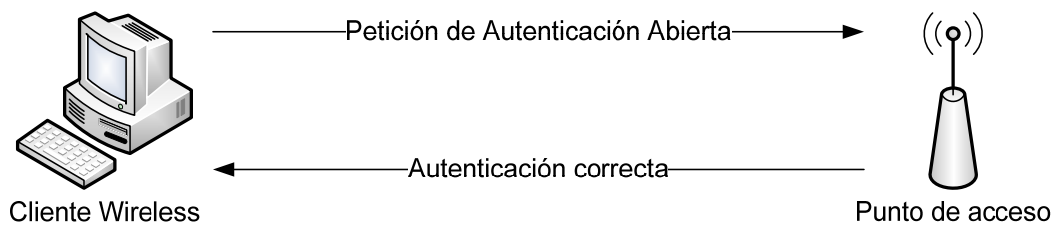


Figura 23. Sistema de autenticación abierta

Shared Key: Clave Compartida

Consiste en un sistema de desafío/respuesta con cifrado WEP entre el cliente y el punto de acceso contra el que desea autenticar. Para lo cual es necesario que ambos elementos utilicen la misma clave.

1. El proceso de autenticación lo inicia el cliente enviando una trama (*management frame*) que le indica al punto de acceso que el método a usar es clave compartida.
2. El punto de acceso responde con el desafío que debe resolver el cliente. Este desafío se genera pseudo-aleatoriamente mediante un algoritmo PRNG (*Pseudo-Random Number Generator*) utilizando la clave compartida y un vector de inicialización.
3. Cuando el cliente recibe el desafío, lo cifra mediante WEP utilizando la clave compartida y un nuevo vector de inicialización elegido por el cliente, y se lo devuelve al punto de acceso.
4. El punto de acceso al recibir esta trama la descifra, comprueba la integridad mediante el CRC y verifica el desafío. Si todo es correcto, se procede a autenticar al cliente.
5. A continuación, se realiza el mismo procedimiento de manera inversa. De tal forma que ambos elementos son autenticados de manera mutua.

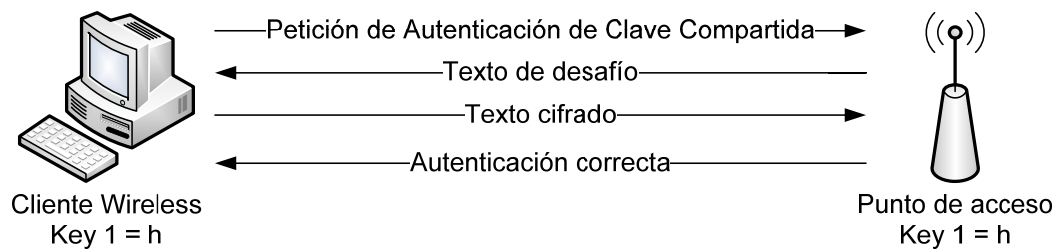


Figura 24. Shared Key: Clave Compartida

Como hemos visto, para poder utilizar este tipo de autenticación, la red debe emplear el protocolo de cifrado WEP.

Su principal vulnerabilidad es que con un software analizador de red es relativamente sencillo obtener los datos para llegar a recrear las tramas necesarias para engañar al punto de acceso,

Basta con capturar el tráfico generado cuando un equipo se autentica en la red, obteniendo el texto de desafío y la respuesta de texto cifrado se consigue todo lo necesario para realizar el ataque.

CNAC: Autenticación cerrada (*Closed Network Access Control*)

En este sistema solo se permite acceso a la red a los clientes que conozcan el ESSID de la misma, es decir, el ESSID actúa como si fuera la clave.

Su principal vulnerabilidad, como hemos visto en otros mecanismos, no es el mecanismo en sí mismo, sino la falta de administración del mismo, ya que, en este caso, los fabricantes establecen valores ESSID por defecto que en muchas ocasiones no son modificados por el administrador de la red.

EAP (*Extensible Authentication Protocol*)

Surge como una de las mejoras de seguridad básicas del estándar 802.1x. Está basado en el protocolo PPP (*Point to Point Protocol*), que utiliza como método de autenticación usuario y contraseña, y proporciona un marco generalizado para diversos métodos de autenticación.

El estándar IEEE 802.1x describe el funcionamiento del protocolo EAP en redes LAN (EAPOL, EAP over LANs).

A continuación se explica el flujo de autenticación¹³ utilizando un servidor RADIUS, donde:

- **Supplicant:** Cliente que solicita la autenticación.
- **Autenticador:** Suministrador de servicio una vez la autenticación ha sido realizada con éxito.
- **Servidor de Autenticación:** Servidor encargado de realizar la autenticación.

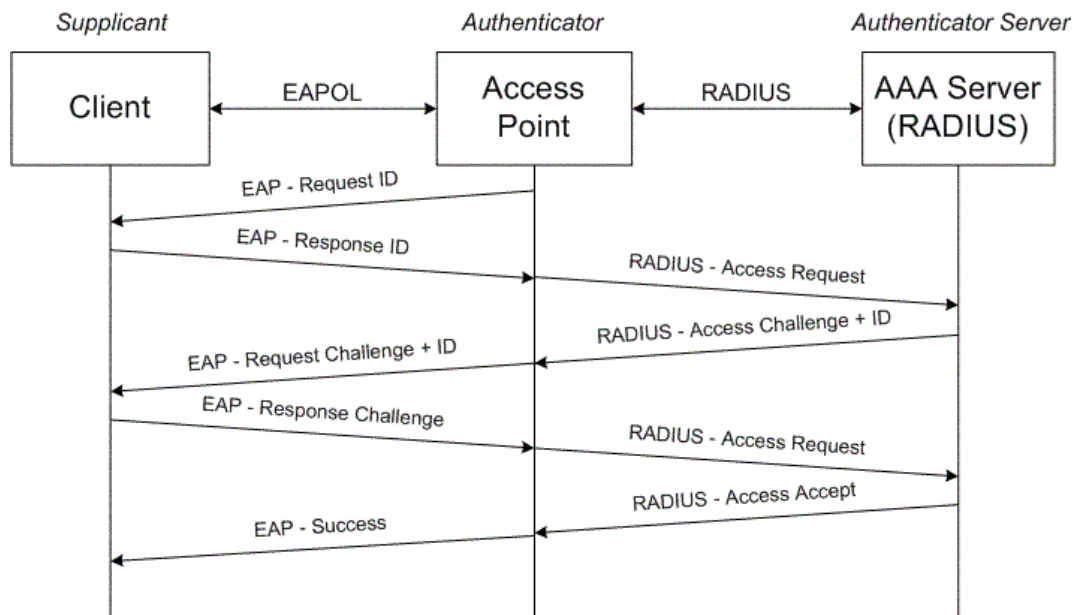


Figura 25. Autenticación EAP

1. El *authenticator* envía un paquete de "*EAP-Request/Identity*" al *supplicant* tan pronto como detecte que el acoplamiento es activo.

¹³ <http://bibing.us.es/proyectos/abreproy/11499/fichero/03+-+Conectividad+de+nuestro+dispositivo.pdf>

2. El *supplicant* envía un paquete de "EAP-Response/Identity" al *authenticator*, que pasa directamente al servidor de la autenticación.
3. El servidor de la autenticación envía un desafío al *authenticator*. El *authenticator* desempaqueta el contenido del paquete IP, lo empaqueta de nuevo en EAPOL y lo envía al *supplicant*.
4. El *supplicant* responde al desafío vía el *authenticator* y pasa la respuesta al servidor de autenticación.
5. Si el *supplicant* proporciona identidad apropiada, el servidor de autenticación responde con un mensaje de éxito al *authenticator*, que es pasado así mismo al *supplicant*. El *authenticator* permite a partir de este momento el acceso al *supplicant*.

Hay una gran variedad de mecanismos de autenticación basados en EAP, algunos son estándares y otras soluciones propietarias de empresas.

Entre los más utilizados están:

- **EAP-MD5:** Se autentifica enviando una cadena cifrada utilizando el algoritmo MD5. Dicha cadena contiene el usuario, contraseña y una cadena arbitraria. El servidor genera su propio MD5, utilizando la clave en texto claro y la cadena arbitraria, y lo compara con el del cliente.

No es muy utilizado ya que usa autenticación simple, no mutua, y además no es compatible con la generación dinámica de claves WEP.

- **EAP-TLS (*Transport Layer Security*):** Autenticación mutua basada en certificados de cliente y servidor. Ofrece compatibilidad con la generación dinámica de claves WEP.

Su principal inconveniente es que son costosos de administrar, ya que requiere la instalación de distintos certificados en todos los equipos y servidores.

- **EAP-TTLS (*EAP Tunneled TLS*)**: Es una extensión de EAP-TLS, que simplifica la gestión, ya que requiere un único certificado del lado del servidor. Se crea un túnel TLS para transmitir el nombre de usuario y la contraseña, evitando así que se puedan capturar mediante escuchas de la red.
- **PEAP (*Protected Extensible Authentication Protocol*)**: Emplea un único certificado del lado servidor. Se crea un túnel SSL/TLS entre el cliente y el servidor de autenticación, por lo que el intercambio de datos, como usuario y clave están protegidos.

Se necesita instalar el certificado del servidor en cada cliente que desea autenticarse en la red.

- **EAP-FAST (*Flexible Authentication Secure Tunneling*)**: No utiliza certificados, en su lugar, la autenticación mutua se consigue por medio de una PAC (Credenciales de Acceso Protegido).

La PAC puede ser proveerse al cliente de forma manual, o bien de forma dinámica contra el servidor de autenticación. En la provisión automática la autenticación y la entrega de la PAC están protegidas mediante un túnel codificado.

- **LEAP (*Lightweight Extensible Authentication Protocol*)**: Patentado por Cisco, basado en nombre de usuario y contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

5.1.2 Cifrado

WEP (*Wired Equivalent Privacy*)

Es un protocolo de cifrado que forma parte de la especificación 802.11, y como su nombre indica, se diseñó para proveer a la comunicación inalámbrica el mismo nivel de seguridad que una red cableada.

WEP opera a nivel 2 del modelo OSI, es decir a nivel de capa física y de enlace.

Para el cifrado, se aplica el algoritmo RC4 con claves de 64 bits o 128 bits. Aunque en realidad son 40 y 104 bits, ya que los 24 bits restantes se utilizan para el vector de inicialización (VI).

Hay que destacar que la clave utilizada en el algoritmo de cifrado realmente no es la que el administrador ha fijado para la red. Sino que a partir de la clave dada por el administrador se generan cuatro claves de forma automática, de las cuales una será la utilizada.

A continuación se detalla el proceso de generación de claves:

1. A la clave fijada por el administrador de la red, denominada My Passphrase, se le aplica una operación XOR, resultando una semilla de 32 bits.
2. Esta semilla se utilizará como entrada del algoritmo generador de números pseudoaleatorios (PRNG) obteniendo 40 cadenas de 32 bits.

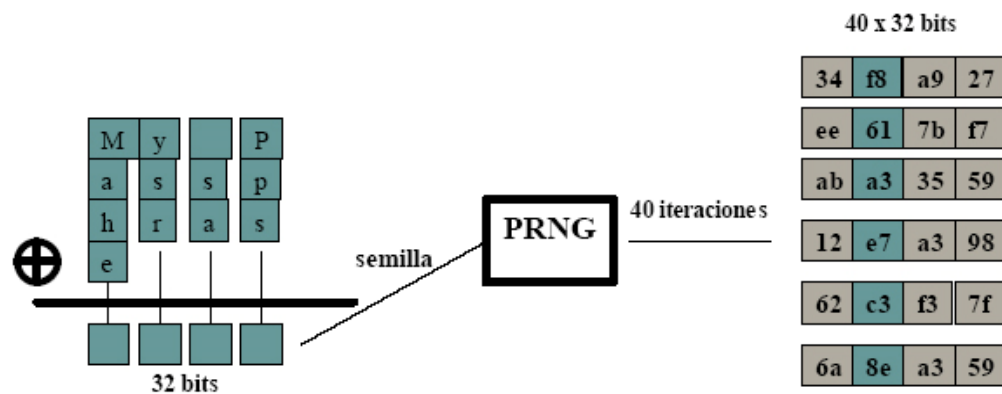


Figura 26. Generación clave WEP

- Para cada una de esas cadenas se toma un bit, y se genera así una clave de 40 bits. Este proceso se hace en cuatro ocasiones, resultando 4 claves de 40 bits cada una.

Algoritmo de cifrado

Una vez se han generado las 4 claves, se utilizará una de ellas en el algoritmo de cifrado de la siguiente manera:

- Se tiene la trama que se desea enviar, la cual está compuesta por una cabecera (*Header*) y unos datos (*Payload*). El primer paso es calcular el CRC de 32 bits de los datos. El CRC añade a la trama, denominándose valor de chequeo de integridad ICV (*Integrity Check Value*), y como su nombre indica, se utilizará para verificar la integridad de los datos, es decir, que los datos que ha recibido son los mismos a los mismos que se enviaron en origen.

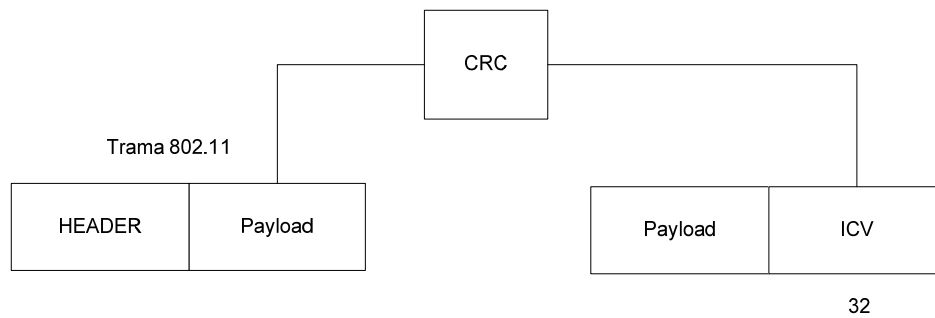


Figura 27. Cifrado WEP. Cálculo de CRC

2. Se selecciona aleatoriamente una de las 4 claves de 40 bits:

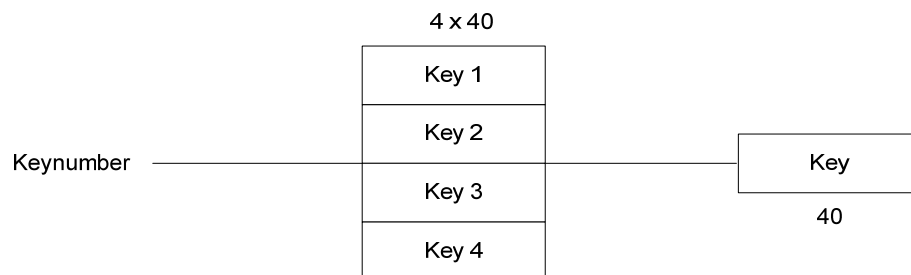


Figura 28. Cifrado WEP. Selección de clave

3. A la clave seleccionada se le añaden 24 bits en lo que se denomina vector de inicialización (IV) que normalmente es un contador que varía según se van generando tramas. Esto se hace con el fin de evitar que el uso de la misma clave resulte en que para dos tramas en claro iguales se produzcan las tramas cifradas.

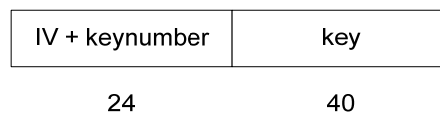


Figura 29. Cifrado WEP. IV + clave

4. Se aplica el algoritmo RC4 a la clave obtenida en el paso anterior, resultando el *keystream*. Y se realiza una operación XOR con este *keystream* y el conjunto *Payload+ICV* obteniendo así el *Payload+ICV* cifrado.

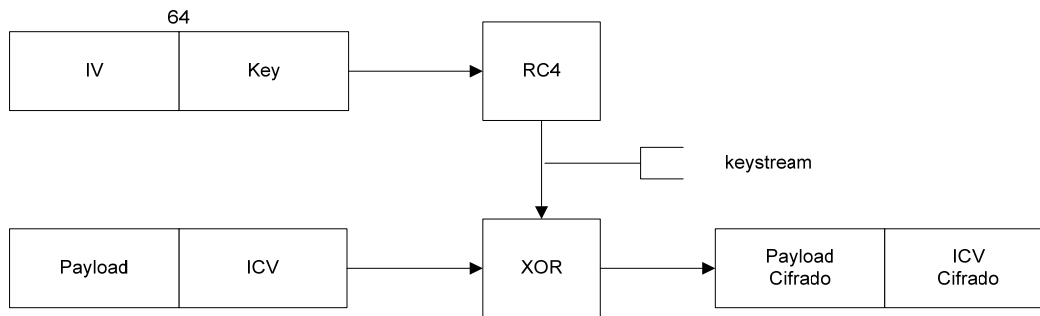


Figura 30. Cifrado WEP. Cifrado del Payload

5. A continuación, para generar la trama a enviar, se le añade la cabecera y el *IV+Keynumber* en claro.

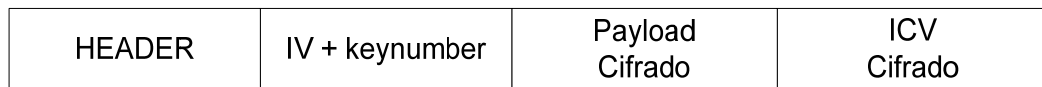


Figura 31. Cifrado WEP. Trama cifrada

Descifrado

A continuación se explica el proceso seguido para descifrar la trama una vez que ha llegado a su destino.

1. Se selecciona, entre las cuatro posibles, la clave que fue utilizada, se sabe porque como hemos visto, el *keynumber* se envía en claro junto con el vector de inicialización.
2. Al principio de la clave se le añade el vector de inicialización, consiguiendo así la clave utilizada en el cifrado.
3. A continuación se aplica el mismo algoritmo que en el cifrado. Este es RC4 a la clave para obtener el *keystream* a aplicar en el XOR que junto con el *Payload+ICV* cifrados darán como salida estos últimos sin cifrar.

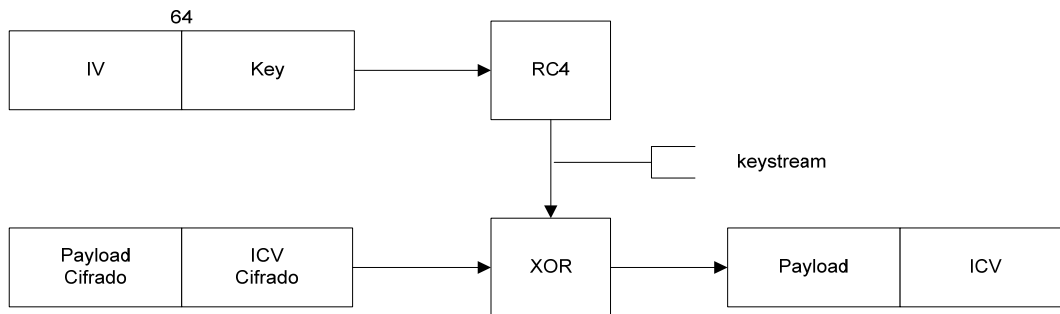


Figura 32. Descifrado WEP. Descifrado del *Payload*

- Una vez obtenido el *payload* como texto en claro se comprueba su integridad. Para ello se calcula su ICV mediante el algoritmo CRC y se compara con el que viene en la trama, si iguales, la trama se acepta, en caso contrario se rechaza.

Deficiencias de WEP

- **Debilidades de CRC32**

Como ya hemos visto, el campo ICV se genera aplicando un CRC (*Cyclic Redundancy Check*) de 32 bits al *payload* a transmitir. Y posteriormente, es utilizado por el receptor como un mecanismo para garantizar la integridad del mensaje.

Sin embargo, el algoritmo CRC tiene dos vulnerabilidades:

- **CRC no depende de la clave:** Los CRCs se calculan a partir del *payload* por lo que son totalmente independientes de la clave utilizada y del IV.

Esto da pie a que se puedan inyectar paquetes en la red con tan solo conocer el *payload* de un paquete cifrado con WEP. El ataque se realizaría de la siguiente manera:

1. Se captura un paquete cifrado del que conocemos el *payload*, por ejemplo mediante el envío de un email a la víctima.
2. A partir del mensaje se recupera el *keystream* $k = c \oplus m$ para el vector de inicialización del paquete.
3. Conociendo el *keystream* y el vector de inicialización (IV), se pueden introducir paquetes para los mensajes deseados m' con CRCs válidos:

$$c = (m' \parallel \text{ICV}') \oplus k$$

$$\text{donde } \text{ICV}' = \text{CRC32}(m')$$

- **Los CRCs son lineares:** $\text{CRC}(m \oplus k) = \text{CRC}(m) \oplus \text{CRC}(k)$

Esta debilidad permite que se puedan modificar los mensajes interceptados generando ICV válidos para ellos.

Esta técnica se denomina *bit flipping*, y se aplica con unos sencillos pasos:

1. Partiendo de un mensaje interceptado m , se modifica de forma conocida para producir m' :

$$m' = m \oplus D$$

2. Al ser CRC-32 lineal, se puede generar un nuevo ICV' válido a partir del ICV de m :

$$\text{ICV}' = \text{ICV} \oplus \text{CRC32}(D)$$

3. ICV' será válido para el nuevo texto cifrado c'

$$c' = c \oplus D = k \oplus (m \oplus D) = k \oplus m'$$

- **Debilidad en la autenticación**

Como ya hemos visto, WEP utiliza uno de los dos sistemas básicos de autenticación:

- **Autenticación abierta:** No existe servicio de autenticación. Basta con conocer la clave WEP para que la comunicación pueda llevarse a cabo. Por lo que cualquier cliente que conozca la clave podría conectarse a la red.
- **Clave compartida:** Es fácilmente salvable realizando escuchas de la red. Con la captura del desafío en claro enviado por el punto de acceso y la respuesta del cliente con el desafío cifrado, ya dispondríamos de todos los elementos necesarios para realizar la autenticación mediante la fórmula: $WEP = \text{Datos cifrados} \oplus \text{Datos}$.

- **Claves estáticas**

El protocolo WEP no proporciona funciones para el intercambio automático de claves entre equipos de la red. Cualquier cambio de clave debe ser administrado manualmente en todos los puntos de acceso y equipos que se conectan a él. Por lo que, habitualmente la clave no se cambia nunca, o muy de vez en cuando.

Esto posibilita que un atacante capture mucho tráfico cifrado con la misma clave, pudiendo realizar un ataque por fuerza bruta.

- **Debilidades en el vector de inicialización**

El estándar 802.11 especifica que cambiar el vector de inicialización en cada paquete es opcional. Lo más habitual es utilizar un contador que empieza en cero y se va incrementando de uno en uno en cada paquete.

- **Tamaño demasiado corto:** El vector de inicialización tiene sólo 24 bits, por lo que existen 2^{24} (16.777.216) posibles valores.

Este número de paquetes pueden llegar a generarse en poco tiempo en una red con un tráfico intenso.

- **Reutilización:** Es un problema derivado de la misma corta longitud del vector de inicialización, al existir tan pocas posibilidades, hace que el valor se repita frecuentemente, propiciando que se puedan realizar ataques denominados estadísticos analizando los paquetes con el mismo vector de inicialización. Se realiza de la siguiente manera:

1. Si tenemos que T, T' son textos que serán cifrados a partir del mismo vector de inicialización.
2. El *keystream* es K = RC4 (clave, IV).
3. Aplicando el algoritmo WEP tenemos los cifrados C y C':

$$C = T \oplus K$$

$$C' = T' \oplus K$$

4. Se puede deducir que:

$$C \oplus C' = (T \oplus K) \oplus (T' \oplus K) = (K \oplus K) \oplus (T \oplus T') = T \oplus T'$$

5. De esta forma si conocemos uno de los textos en claro, se puede deducir el otro estadísticamente.

WPA (WiFi Protected Access)

Surge como respuesta a las vulnerabilidades encontradas en WEP. Se trata de una serie de medidas temporales mientras se trabajaba en finalizar el estándar IEEE 802.11i.

Aporta mejoras sustanciales en la seguridad en diferentes aspectos, como son autenticación, cifrado e integridad de la información.

Además, ya que no requiere de gran capacidad de procesamiento, es posible mantener la compatibilidad con el hardware utilizado hasta el momento en WEP mediante una actualización del firmware.

Autenticación

El protocolo WPA define dos métodos de autenticación diferentes:

- **IEEE 802.1X (Servidor de autenticación).** Permite control de acceso a la red basado en puertos. Los clientes intentan la conexión al punto de acceso a través de un puerto, el cual se mantiene bloqueado hasta que se considere al usuario autenticado. Para realizar esta autenticación se utiliza el protocolo EAP y requiere de un servidor de autenticación denominado AAA (*Authentication Authorization Accounting*), habitualmente se utiliza como tal un RADIUS.

Es la opción más segura, pero es una solución costosa, por lo que este modo está principalmente indicado para el uso empresarial.

Con clave inicial compartida (PSK). No requiere servidor de autenticación, para la autenticación se utiliza una clave compartida entre los dispositivos y el punto de acceso. Esta clave sólo es utilizada para realizar la autenticación, no para el cifrado de los datos.

Su uso está recomendado para entornos domésticos y pequeñas redes.

Cifrado

WPA emplea claves dinámicas para el cifrado, de tal manera que la clave utilizada cambia constantemente, cada paquete está cifrado con una clave diferente de los anteriores. Para ello utiliza el protocolo de integridad de claves temporales (TKIP *Temporal Key Integrity Protocol*)

Sin embargo se han detectado vulnerabilidades en este mecanismo, no por debilidad propia del sistema, sino derivados de una mala elección de la clave preestablecida. De tal forma que si se utilizan palabras comunes, que puedan estar presentes en un diccionario de un atacante y además la longitud de la misma es menor a 20 caracteres, basta con interceptar el tráfico inicial generado en el intercambio de claves para poder obtener dicha clave mediante un ataque de diccionario.

Por lo que si se realiza una mala elección de la clave inicial, el protocolo WAP podría ser roto incluso más fácilmente que WEP, ya que para poder sacar las claves de este, es necesario capturar un gran volumen de tráfico, mientras que en WPA es suficiente con capturar el tráfico de intercambio de claves.

Chequeo de la integridad de la información

Dadas las vulnerabilidades encontradas en el algoritmo CRC que utiliza WEP para comprobar la integridad de los mensajes, en WPA se define un nuevo método para reemplazarlo denominado MIC (*Message Integrity Check*), el cual ha sido diseñado específicamente para evitar que los mensajes sean fácilmente alterables como ocurría con CRC.

Este método, también conocido como *Michael*, consiste en un *hash* criptográfico de un solo sentido. Este se calcula utilizando la dirección física origen y destino y *payload* después de ser segmentado por la llave MIC y el TSC.

El destinatario comprueba que el TSC del paquete recibido tiene mayor valor que el anterior. En caso contrario el paquete se descarta evitando así ataques por repetición.

Después de que el valor del MIC sea calculado basado en el MSDU recibido y cifrado, el valor calculado del MIC se compara con el valor recibido.

- Un Vector de Inicialización (IV) de 48 bits llamado TSC (*TKIP sequence counter*) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La estructura de cifrado TKIP propuesta por 802.11i sería la siguiente:



Figura 33. Paquete cifrado TKIP

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 248 paquetes utilizando una sola llave temporal antes de ser rehusada.

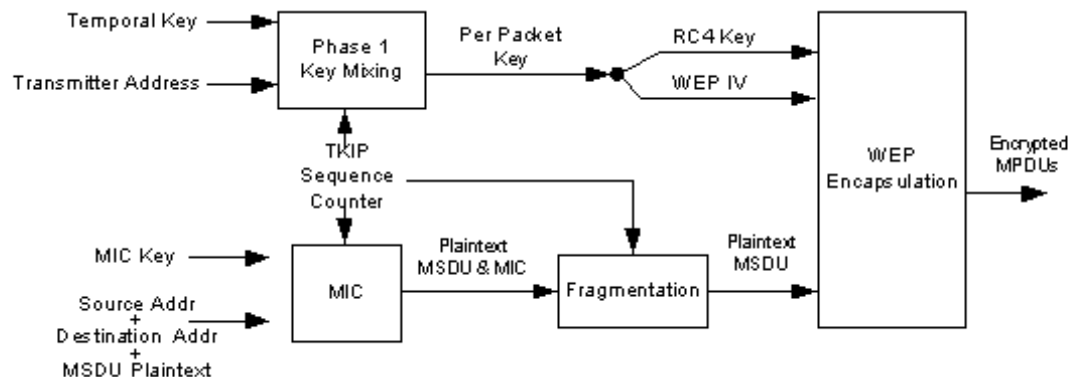


Figura 34. Cifrado TKIP

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV de 24 bits para su posterior encapsulación WEB.

WPA2 (IEEE 802.11i)

802.11i es, hasta el momento, el último estándar del IEEE pensado para proporcionar mayor seguridad a las redes inalámbricas.

WPA2 es el protocolo que lleva la implementación completa del estándar. Introduce principalmente dos mejoras respecto al protocolo WPA:

• Algoritmo de cifrado AES (*Advanced Encryption Standard*)

Fue desarrollado por el Instituto Nacional de Estándares y Tecnología de EEUU (NIST por sus siglas en inglés).

Es un algoritmo de cifrado de bloque, se basa en una serie de sustituciones, permutaciones y transformaciones lineales ejecutadas en bloques de 16 bytes que se ejecutan en varias rondas. La modificación de un único bit, ya sea en la clave o en los bloques da como resultado un texto cifrado totalmente diferente

Existen versiones con claves de 128, 192 y 256 bits. En la actualidad, se considera a AES como uno de los algoritmos de cifrado más potentes que existen y hasta el momento no se le conoce ningún punto débil. Por poner un ejemplo, en recientes investigaciones, se considera que para romper AES de 128 bits con un superordenador actual, harían falta unos 2.000 millones de años.

Como único inconveniente destacable es que al ser un algoritmo muy complejo, necesita un gran número de cálculos por lo que las necesidades de hardware aumentan respecto a los cifrados que se usaban anteriormente. Este punto es considerable ya que los dispositivos más antiguos no tienen capacidad para procesar esos cálculos por lo que no introducen AES mediante actualizaciones de firmware.

Además, WPA2 incluye soporte para redes en modo IBSS (redes ad hoc), y no solo para modo BSS (infraestructura) como WPA.

•Uso de CCMP para garantizar la integridad de los mensajes

Para asegurar la integridad de los mensajes se sustituye el uso de códigos MIC por el protocolo CCMP.

Este protocolo es complementario al TKIP representa un nuevo método de cifrado basado en AES, cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC.

Utiliza un IV de 48 bits denominado Número de Paquete (PN), junto con la información para inicializar el cifrado AES para calcular el MIC y el cifrado de la trama.

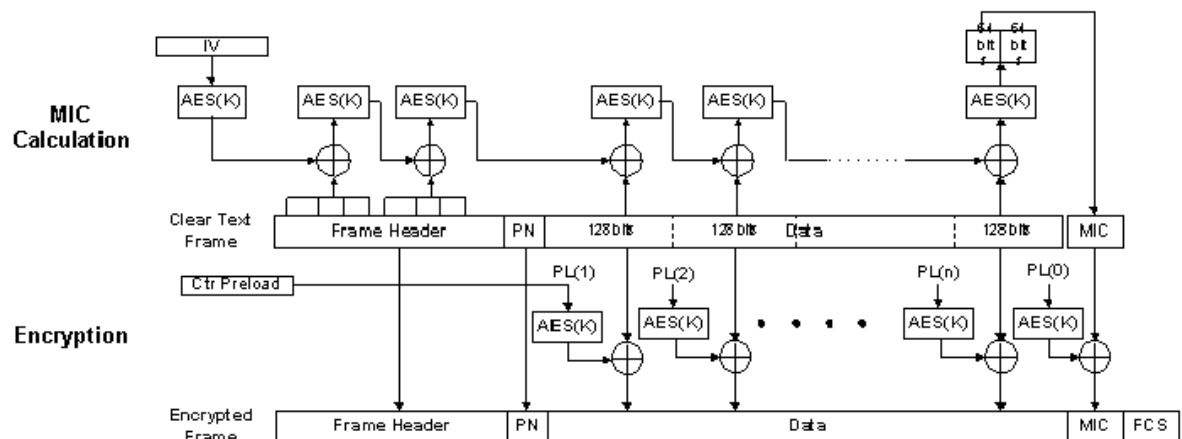


Figura 35. Cifrado CCMP

En el proceso de cifrado CCMP, el cifrado de los bloques utiliza la misma clave temporal tanto para el cálculo del MIC como para el cifrado del paquete.

Al igual que en TKIP, la clave temporal se deriva de la clave principal obtenida como parte del intercambio en 802.1x.

El cálculo del MIC y el cifrado se realiza de forma paralela. El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.

5.1.3 Control de acceso

SSID (*Service Set Identifier*)

El SSID (*Service Set Identifier*) es un código que se incluye en todos los paquetes que se transmiten en una red inalámbrica para poder identificarlos como tráfico de la red, por lo tanto todos los dispositivos que se comuniquen entre sí dentro de la misma red deben conocer el mismo SSID.

Comúnmente el SSID es lo que todos conocemos como el nombre de la red.

El SSID tiene dos posibles variantes según el tipo de red del que se hable:

- BSSID (*Basic SSID*) en redes ad-hoc
- ESSID (*Extended SSID*) en redes infraestructura

Una buena práctica para evitar el acceso a la red, es ocultarla desactivando la propagación del SSID. De este modo la red no se verá como disponible, y tan solo se podrán conectar a ella conociendo de antemano su ubicación y SSID.

Autenticación por MAC

Habitualmente los puntos de acceso permiten configurar listas de control de acceso (ACLs) basándose en la dirección física de los dispositivos cliente, o lo que es lo mismo por su dirección MAC.

El punto de acceso utiliza la lista como mecanismo de autenticación, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista.

Su principal debilidad es que las direcciones MAC se envían en claro en la comunicación, por lo que escuchando la red se pueden capturar direcciones permitidas por el punto de acceso. Teniendo una dirección válida, se puede suplantar su identidad modificando la interfaz de la tarjeta de red.

Capítulo 6

Auditoría

6.1 Introducción

6.1.1 Auditoría en general

Según la definición de William Thomas Porter:

“Auditoría es el examen de la información por terceras partes, distintas de quienes la generan y quienes la utilizan, con la intención de establecer su suficiencia y adecuación, e informar de los resultados del examen con objeto de mejorar su utilidad.”

En otras palabras, se puede decir que auditar consiste en comparar lo que se hace frente a lo que se debería hacer y lo que existe frente a lo que debería existir. Es un análisis de las deficiencias de un entorno o sistema, dando como resultado un informe con una serie de recomendaciones para subsanarlas.

6.1.2 Auditoría informática

La auditoría informática abarca la revisión, análisis y evaluación de sistemas, programas, entornos y cualquier aspecto relacionado con la informática, por parte de personas objetivas e independientes que poseen los conocimientos técnicos suficientes en el entorno que se pretende auditar.

El resultado de ese trabajo se plasma en un informe que debe contener la situación del entorno auditado, las deficiencias encontradas, así como recomendaciones para subsanarlas.

Hoy en día, la información es un activo que ha adquirido una gran importancia para la gestión de cualquier entidad, considerándose uno de los principales activos de estas.

Por ello, existe cada vez más, la necesidad de ejercer un mayor control, y de la realización de auditorías informáticas internas y externas.

6.2 Tipos de auditoría informática

La auditoría informática puede cubrir muchos aspectos, dependiendo del objetivo de la auditoría.

Habitualmente un proceso de auditoría abarca varios de los siguientes aspectos:

- Verificación de controles: Evaluación del sistema de control interno por parte de la auditoría interna o evaluación de la auditoría interna por parte de la auditoría externa.
- Auditoría de cumplimiento: de políticas, estándares y procedimientos de la propia entidad, de normas legales aplicables, de acuerdos inter-empresas...
- Auditoría de seguridad: Tanto física como lógica.
- Auditoría de calidad: Verifica se cumplen las políticas y requisitos de calidad mínima impuestos por la entidad.
- Auditoría operativa: Como se están haciendo las cosas.
- Auditoría de gestión: Eficiencia/eficacia, posibles mejoras en cómo se hacen las cosas.
- Apoyo a la auditoría de cuentas: Para garantizar que el proceso de los datos (a lo largo de todo su ciclo de vida) y los programas que los manejan son los adecuados, y están razonablemente exentos de error y de fraude.
- Apoyo a auditorías específicas de aspectos fiscales.
- Auditorías policiales: Abarcan la investigación de algún delito (siendo los recursos informáticos el medio o el fin).

- Auditorías de RRHH: Relacionadas con las funciones de personal, sus riesgos, sus niveles de satisfacción, su rotación, promoción, condiciones de trabajo y ergonomía.
- Auditorías especiales, relacionadas con la compra de una entidad por otra o fusión inter-empresas.
- Auditorías de cumplimiento: Verifican el cumplimiento de leyes y normativas, como pueden ser LOPD, ENS e incluso de la LSSI.

Para cumplir con todo ello, se tienen tres líneas de defensa, cuyos cometidos se complementan, pudiendo ser necesarias las tres:

6.2.1 Control interno

Actividad o acción realizada por uno o varios elementos para prevenir / detectar / corregir errores o irregularidades que afecten al funcionamiento de algo. Realizado por supervisores de distinto nivel, debe producirse en el día a día. En el caso de informática lo realizan jefes de proyecto, jefes de turno, etc.

A mayor control mayor fiabilidad. Si se demuestra que los controles son efectivos, las partes interesadas / afectadas por la Informática de una entidad tendrán una confianza razonable en los sistemas y en los datos.

Es difícil saber cuánto control es necesario aplicar, para a la vez que se garantiza una situación razonablemente fiable no se disparen los costes y no disminuya la productividad. Frente a ello, es necesario evaluar los riesgos derivados de la inexistencia del control.

La implantación de los controles es una responsabilidad de la Dirección, si bien cada directivo en su área es corresponsable de la existencia de controles al nivel determinado. La existencia de estos controles, así como su eficiencia e idoneidad, es verificada por los auditores, comunicando de forma objetiva a través de los informes las deficiencias, los riesgos y las posibles mejoras de

estos. Así mismo se puede recomendar que se implanten o refuercen ciertos controles, al igual que en contadas ocasiones, se puede sugerir la supresión de los mismos, siempre y cuando se justifique que ya no son necesarios.

Características de los controles

Para garantizar la buena función de los controles deben cumplir las siguientes características:

- | | | |
|-------------|--------------|--------------|
| ○ Simples | ○ Razonables | ○ Fiables |
| ○ Prácticos | ○ Operativos | ○ Rentables |
| ○ Completos | ○ Adecuados | ○ Revisables |

Debe evaluarse la rentabilidad, considerando el coste de implantación de los controles (coste de mantenerlos + coste de hacer seguimiento de los mismos) versus el coste de no implantar los controles.

Tipos de controles:

- **Directivos:** Crean el marco de actuación, definiendo las políticas.
- **Preventivos:** Se realizan antes del hecho, para evitar que ocurra.
- **De detección:** Seguimiento de controles preventivos. Reflejan acciones contra normas o prácticas.
- **Correctivos:** Para rectificar errores, y para salvar situaciones producidas por omisiones.
- **De recuperación:** Facilitan la vuelta a la normalidad después de haberse producido errores o interrupciones.

6.2.2 Auditoría interna

El acceso a personal, ficheros, documentos, contratos, actas, etc., ha de ser suficiente para poder investigar y realizar informes objetivos e independientes, que puedan hacer llegar a quienes no estén implicados en los procesos auditados.

No debería depender del Director de Informática ni de ninguno de sus colaboradores. Puede depender del jefe del Director de Informática, del Director General o del Auditor General.

Es deseable que exista un Comité de Auditoría; si no, el Comité de Sistemas de Información o el propio Comité de Dirección, actuarán como tal mediante decisiones sobre la auditoría informática (desde la creación de la función) y estar al tanto de los resultados.

Si existe el Comité de Auditoría, debe estar presidido por el ejecutivo del máximo nivel y formar parte de él los directivos de todas las áreas de la entidad.

Este comité, de forma colegiada o a través de su presidente, encargará las auditorías que considere necesarias y/o aprobará el plan presentado por Auditoría Informática.

Creación de la función de Auditoría Informática Interna:

Una vez clarificados los aspectos de dependencia han de seleccionarse las personas, existen dos opciones:

- Auditores proceden de la propia plantilla de la entidad, tendrá ventajas en cuanto a que son personas conocidas y que conocen el entorno a auditar, así mismo se sabe la formación de estos, y si están capacitados para desempeñar la auditoría. Pero también existen inconvenientes de que el auditor proceda de la propia plantilla, como puede ser su relación de amistad con los auditados, lo cual le impediría ser objetivo e independiente.

- En el caso en que los auditores internos sean contratados del exterior, estos deberían tener experiencia en entornos afines al entorno a auditar, lo cual facilitará su trabajo, siendo también una auditoría más completa y fiable.

6.2.3 Auditoría externa

A pesar de que aún no existe una normativa ni la obligatoriedad de realizar este tipo de auditorías informáticas, si existe tal para la Auditoría de Cuentas, y dada la necesidad de garantizar que el proceso de los datos se realiza con los suficientes y necesarios controles, se suele realizar una auditoría informática unida a la auditoría de cuentas. Ambas auditorías deben ser realizadas por personas distintas, dada la necesidad de especialización en cada sector.

La auditoría informática externa normalmente será encargada por la Dirección General, por el Consejo de Administración, o incluso directamente por una mayoría de accionistas.

Existe obligatoriedad de someterse a la Auditoría de Cuentas externa las entidades que:

- Emitan obligaciones en oferta pública.
- Sus títulos coticen en bolsa.
- Se dediquen de forma habitual a la intermediación financiera, al igual que las entidades financieras que deban estar inscritas en los correspondientes Registros del Ministerio de Economía y Competitividad y Hacienda y Administraciones Públicas y del Banco de España.
- Tengan por objeto social cualquier actividad sujeta a la Ley de Ordenación del Seguro Privado.

- Reciban subvenciones, ayudas o realicen obras, prestaciones, servicios o suministren bienes al Estado y demás Organismos públicos dentro de los límites que reglamentariamente fije el Gobierno por Real Decreto.
- Las empresas, sociedades cooperativas y entidades que superen los límites que reglamentariamente fije el Gobierno por Real Decreto (dichos límites se referirán al menos a cifra de negocios, importe total del activo y número medio anual de empleados).

Debe realizarse una contratación formal que especifique el alcance del proceso de auditoría, el ámbito geográfico, las características del proceso a realizar, los resultados a obtener (el tipo de informe), el marco temporal, el precio a abonar (y las condiciones y forma de pago).

También será necesario en su caso, especificar cláusulas de confidencialidad, así como el compromiso de aceptar las normas internas del cliente en lo que respecta a la seguridad. Igualmente pueden incluirse cláusulas adicionales que especifiquen aspectos como el acceso a datos y personal que dispondrán los auditores, de cómo tratar las posibles divergencias que surjan, y otras tales referentes a la relación entre la entidad auditada y el auditor, por ejemplo que los auditores no contraten a personal del cliente ni viceversa hasta pasado un tiempo después de la finalización del trabajo.

Es muy recomendable que exista un plan del trabajo a realizar, para tener organizado y a disposición del auditor todo lo requerido a tiempo para realizar su trabajo, sin que por ello se evite el factor sorpresa cuando sea necesario.

6.3 El auditor informático

La procedencia del auditor informático, siempre ha habido discrepancia en si se formaba a auditores en informática o a informáticos en auditoría, desde hace unos años se ha venido optando más por esa segunda opción ya que resulta más sencillo que un informático con experiencia y con aptitudes aprenda los principios, técnicas y métodos de la auditoría y control, frente a la opción de que otro profesional de la auditoría, aprenda aspectos de la informática con suficiente profundidad como para desarrollar su trabajo con garantías.

6.3.1 Funciones

Las funciones a realizar por el auditor informático serán las que se determinen para cada entidad, y con diferencias si se trata de auditores internos o externos, estas funciones serán definidas por escrito en el momento de la solicitud de auditoría. Por lo general, las funciones comunes son:

- Realización del trabajo de campo:
 - Entrevistas
 - Pruebas y verificaciones
 - Análisis de la documentación
 - Organización y archivo de los papeles de trabajo
- Propuesta de sugerencias
- Propuesta de recomendaciones
- Colaboración con los jefes de equipo (en el caso de existir un equipo)

6.3.2 Perfil

El auditor informático habrá de tener un nivel suficiente de las siguientes cualidades y requisitos:

- **Formación:** Deberá incluir aspectos de informática, de auditoría y de control, más aspectos complementarios sobre cómo elaborar cuestionarios, como realizar entrevistas y como redactar informes.
- **Experiencia:** Debería estar relacionada con la informática, y más en concreto con el sector a auditar.

Estos dos aspectos son especialmente importantes ya que los auditados, en caso de que el auditor no tenga el nivel necesario, podrían llevarle al terreno que más les convenga, provocando así que el auditor pase por alto muchos aspectos del campo a auditar.

Si el auditor no tiene los conocimientos suficientes para auditar áreas técnicas puede ayudarse de expertos, de la propia instalación o externos, estos a su vez deben actuar de forma objetiva e independiente. Para ello, si son empleados de la propia instalación a auditar, no pueden nunca estar implicados en los procesos que se están auditando.

Otros requisitos importantes que el auditor debe cumplir son:

- **Independencia:** Debe tener una actitud mental que le permita actuar con libertad respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad en la consideración objetiva de los hechos, y en la formulación de sus conclusiones.
- **Integridad:** El auditor siempre debe ser honesto y sincero en el ejercicio de su trabajo y en la realización de su informe. Por lo tanto, todas las actividades que realice han de estar presididas por una honradez profesional intachable.

- **Objetividad:** Implica que debe mantener en todas sus funciones una actitud imparcial. Debe ser justo y no permitir ningún tipo de influencia o prejuicio. Para lo cual, deberá gozar de una clara y total independencia respecto a la entidad auditada.

Además el auditor debe ser seguro de sí mismo, responsable, y tener interés por el trabajo desarrollado, puesto que de lo contrario se dejarán en el tintero muchos aspectos importantes para la buena realización del informe.

Por último destacar, que al dedicarse a un sector en constante actualización, y evolución, el auditor debe tener una constante puesta al día en conocimientos relativos a las nuevas tecnologías surgidas.

6.3.3 Ética

Es imprescindible que la conducta profesional se rija por la ética profesional. Los auditores informáticos asociados a la ISACA tienen un código de conducta profesional:

- Fomentar el establecimiento y cumplimiento de estándares, procedimientos y controles adecuados, en los sistemas de información.
- Cumplir con los Estándares de Auditoría de Sistemas de Información, que han sido adoptados por la ISACF (Fundación de Auditoría y Control de Sistemas de Información)
- Servir con diligencia, lealtad y honradez los intereses de sus empleados, accionistas, clientes y público en general. No participarán conscientemente en ninguna actividad ilegal o impropia.
- Garantizar la confidencialidad de la información obtenida en el ejercicio de sus funciones. No se usará dicha información en beneficio propio, ni dejarán que llegue a terceros no pertinentes.

- Cumplir con sus funciones de forma objetiva e independiente, evitando actividades que pongan en entredicho (o lo parezca) su independencia.
- Mantener la competencia en los campos interrelacionados de la auditoría y los sistemas de información, mediante su participación en actividades de desarrollo profesional.
- Aplicar el debido cuidado para obtener y documentar pruebas objetivas suficientes, en que basar sus conclusiones y recomendaciones.
- Informar a las partes interesadas sobre los resultados del trabajo de auditoría efectuado.
- Fomentar la formación de directivos, clientes y público en general, para que mejore su entendimiento de lo que son la auditoría y los sistemas de información.
- Mantener altos estándares de conducta y comportamiento personal en sus actividades, tanto profesionales como privadas.

6.3.4 Métodos, técnicas y herramientas

Como se comentó con anterioridad, el realizar una auditoría informática no implica que para ello se requiera el uso del ordenador, es más, la mayoría del trabajo realizado por el auditor informático se realizará con métodos y técnicas que no precisan la utilización de estos (aunque es posible que se apoyen en ellos para facilitar la organización de los datos entre otras tareas), este tipo de técnicas se denominan clásicas, mientras que las técnicas realizadas con el uso de ordenadores se denominan avanzadas.

Vamos a ver a continuación las técnicas más comunes realizadas en este tipo de auditorías:

Cuestionarios

El cuestionario sigue siendo válido y necesario en la auditoría informática, ya que aunque se realice con ayuda de un ordenador y en él se tecleen las respuestas, su esencia es la misma.

Cuando hablamos de cuestionarios nos estamos refiriendo tanto a cuestionarios-guía que ayudan al auditor en su trabajo, a listas de comprobación o de verificación, como a aquellos cuestionarios que el auditor puede entregar al auditado para que responda y después comentar.

En ocasiones un mismo cuestionario se puede usar para dos cosas: uso del propio auditor, y para que lo rellene el auditado, pero en cuanto a su diseño deben ser diferentes, y el pensado para que lo conteste el auditado sin estar presente el auditor debería ser fácil de entender e incluir explicaciones para usuarios, es muy conveniente que después haya una entrevista para comentar y aclarar algunos puntos.

Es fundamental que el auditor entienda perfectamente las preguntas y todo su alcance; si el entrevistado pide aclaraciones y el auditor no es capaz de darle una respuesta razonable el efecto es negativo, y al final se dudará incluso de la validez del informe, del diagnóstico y de las posibles recomendaciones.

Existen varios tipos de cuestionarios:

- **Simple:** Cuando las respuestas no requirieren cuantificación. Si hicieran falta explicaciones adicionales se pueden incluir en hojas adicionales y relacionarlas con una llamada.
- **De respuestas cuantificables:** Pueden usarse barras numéricas o asignar una casilla donde se rellene el valor correspondiente.
- **Matrices**

Entrevista

Es un diálogo entre el auditor y el auditado. Excepcionalmente puede haber varios entrevistados a la vez, pero esto les impedirá hablar con claridad y les puede permitir arroparse el uno al otro.

Es posible que haya más de un auditor para reforzar, pero esto no es demasiado conveniente, ya que puede aturdir al auditado dándole la sensación de interrogatorio. Esto tan solo suele ser realizado cuando uno de los auditores no tiene suficiente experiencia; pudiendo incluso al principio realizar las preguntas el auditor experto, quedando el inexperto tan solo tomando notas.

- **Preparación**

Debería analizarse previamente si la información a averiguar no está disponible por otros medios, a fin de evitar molestar al entrevistado, salvo que se quieran contrastar opiniones o simplemente disponer del testimonio o confirmación por parte del entrevistado.

Una vez elegidas las funciones a entrevistar, es recomendable entrevistar a varias personas de una misma función para contrastar. Lo ideal es que el auditor pudiera elegirlos, pero es de esperar que los auditados traten de que se entreviste a determinadas personas e intentarán evitar que se entreviste a otras (los descontentos, conflictivos, etc.).

Es bueno conocer previamente unos cuantos detalles sobre los entrevistados, aspectos como su personalidad y situación en el organigrama de la empresa, su trayectoria y su grado de integración en la entidad, para así saber la validez de las respuestas y en su caso aplicar algún coeficiente corrector.

Respecto a la hora de la entrevista, es conveniente evitar la hora de la comida, y el tiempo inmediatamente posterior, siendo lo más conveniente la media mañana, cuando el entrevistado está despejado y ha tenido tiempo de resolver los asuntos más urgentes del día. En algunos casos excepcionales, es conveniente comer con el entrevistado para conseguir así mayor información.

En cuanto al lugar de la entrevista, si el despacho o puesto de trabajo del entrevistado no permite la confidencialidad o tranquilidad necesarias y se producen interrupciones continuas, es preferible utilizar un despacho o sala de reuniones aislados e idóneos.

Es muy conveniente enviar con antelación una carta o nota a la persona a entrevistar, e incluso incluir en ella los puntos que se van a revisar. Esto facilitará el trabajo si bien se suprime el factor sorpresa, que en algunos casos es imprescindible.

- **Realización**

En la introducción hay que intentar tranquilizar al entrevistado sin quitarle rigor ni importancia al proceso.

No debe grabarse la conversación, ya que ello casi seguro que pondrá nervioso al entrevistado y le dará la sensación de interrogatorio, salvo que tengamos su autorización. Tampoco se deben tomar demasiadas notas, tan solo escribir lo fundamental incluso con abreviaturas; para evitar esto, en muchos casos se pueden tener las preguntas preparadas de forma que baste con seleccionar una o varias respuestas, anotar un porcentaje, etc.

Es imprescindible que el auditor tenga una base técnica-informática suficiente para entender qué le dicen, y evitar que el entrevistado le lleve al terreno que más le convenga. En resumen, los auditados y auditores deberían huir de la jerga técnica.

El auditor no debe dar la sensación de que está acusando de nada al entrevistado o de que está sometiéndolo a una serie de preguntas buscando que falle algo, como si ese fuera su único cometido para justificar la auditoría.

- **Qué evitar**

El auditor no debe anticipar las respuestas ni inducir en su pregunta a una respuesta determinada.

No hay que intercambiar los roles, lo que ocurre a veces cuando el auditor asume el papel del auditado, sobre todo cuando el auditor ha sido previamente informático y asocia situaciones a otras vividas por él. También puede ocurrir cuando el auditado se considera más preparado que el auditor o ha asistido a seminarios o leído publicaciones especializadas.

El auditor no debe dar consejos “off the record”, y debe dejar claro que las únicas opiniones y recomendaciones válidas por su parte son las contenidas en el informe oficial final.

- **Qué más hacer**

Es muy importante estar al tanto de las reacciones del entrevistado ante las preguntas o cuando llega a determinados puntos. El auditor deberá interpretar cualquier gesto, sofoco, silencio o cambio de postura del entrevistado.

A veces los auditados quieren dar a entender algo que no se atreven a manifestar abiertamente, esos mensajes hay que saberlos captar y tratar de interpretarlos y contrastarlos.

Analizar la entrevista lo antes posible para iniciar el informe. Es imprescindible separar en el informe los hechos de las opiniones.

- **Observación**

La situación ideal es la que se produce cuando como auditores observamos y no saben que lo somos. Esto es complicado si no existe el factor sorpresa, ya que los auditados, aunque no sepan quién es el auditor, saben que están en el lugar, con lo que esos días los auditados cumplen mejor las normas.

Sirve de manera muy especial para rebatir las afirmaciones en una entrevista.

Flujogramas

Ayudan a representar procesos, por lo que pueden ser de gran utilidad a los auditores para interpretar los procesos realizados, o elaborarlos ellos mismos.

Permiten plasmar los sistemas de información y sus componentes manuales e informatizados, y en las distintas plataformas: equipos centrales, terminales...

Muestreo estadístico

En función del análisis de un muestreo el auditor decidirá si debe analizar una muestra más amplia o considera que el resultado es satisfactorio.

El examen ideal (fiabilidad del 100% si suponemos que no se produce ningún error) sería el que comprendiera el 100 de la “población”, y en la medida en que el porcentaje fuera mayor, mayor sería también la fiabilidad, pero hay que considerar el punto de equilibrio en el que con un coste mínimo se tenga una fiabilidad suficiente.

Comunicaciones escritas

Se refiere a las notas o memoranda que los auditores escribirán con diferentes propósitos, no a las que los auditores enviarán a los auditados, ni al informe.

La estructura varía en función del objetivo pero en todo caso es necesario tener unos estándares para que otras personas del equipo o de la entidad auditora puedan interpretar fácilmente las comunicaciones.

En ocasiones será el propio autor el que tendrá que releer lo que en su día escribió, por ejemplo cuando se produce una nueva auditoría al mismo cliente o centro.

6.4 Papeles e informes

Cuando se realiza un proceso de auditoría se utiliza generalmente mucha documentación, esta se puede dividir en entrada al proceso de auditoría y salida del mismo.

6.4.1 De entrada

Son los que usa el auditor para la realización de su trabajo. Dentro de los documentos de entrada se divide a su vez en dos:

Archivo permanente

Este tipo de archivo lo llevan preferentemente los auditores internos, si bien en el caso de externos puede ser útil si se prevé cierta continuidad para años siguientes.

De un proceso de auditoría concreto

- **Documentación especial recogida/recibida**

No puede considerarse propiamente como papeles de trabajo, puede tratarse de informes de consultores, peticiones de usuarios a Informática... documentación que en algunos casos puede pasar a formar parte del archivo permanente.

- **Papeles de trabajo**

Documentación del proceso de auditoría de los procedimientos seguidos, entrevistas, pruebas realizadas, información recogida y conclusiones.

Pueden ser la única defensa del auditor frente a su informe (enlace con el trabajo de campo).

- **Características de los papeles**

- Completos
- Exactos: Es muy conveniente que el auditor aclare por escrito como ha verificado las pruebas contenidas en los papeles o que puedan derivarse de estos.
- Claros y fáciles de entender: Siempre que sea posible se deben usar formularios estándar o que al menos respondan a formatos predeterminados. También deben evitarse los papeles manuscritos, que pueden conservarse como anexo pero cuya transcripción a ordenador debe realizarse lo antes posible.
- Numerados y clasificados: Cada papel debe tener un identificador único, y deberían existir varios índices.
- Útiles para justificar el trabajo de los auditores, para que otros revisen las conclusiones del borrador del informe y para formación de “juniors”.
- En cuanto al tiempo que deben guardarse los papeles de trabajo, no existen requerimientos legales al respecto, y lo prudente puede ser conservarlos un mínimo de cinco años.

- **Estructura de los papeles**

Cada entidad se organiza los papeles de trabajo como considera más conveniente para cumplir sus fines; no obstante, se indican algunas líneas de orientación

- Portada:
 - Cliente/Instalación
 - Tipo de trabajo, fechas y número identificativo
 - Personal que intervino y quién aprobó los papeles de trabajo

- Descripción del contenido
- Índices
- Cuerpo:
 - 1. Hoja descriptiva del proyecto
 - 2. Memorando de objetivos concretos
 - 3. Programa de trabajo
 - 4. Resúmenes de tiempos (y gastos)
 - 5. Puntos para el informe
 - 6. Comentarios de gerente/jefe de equipo
 - 7. Segundas revisiones
 - 8. Informe borrador
 - 9. Contestación de auditados al borrador
 - 10. Informe definitivo
 - A-0. Cedula sumaria (objetivo general)
 - A-1. Objetivo particular número 1
 - A-n/m. (Hoja número m del borrador n)

6.4.2 De salida (el Informe)

Valoración por escrito de la situación general o de un área, indicando las debilidades de control interno, riesgos y posibles mejoras. Este informe es la comunicación formal con los auditados y la dirección.

Después de todo el proceso de auditoría, el informe es el único producto perdurable, y por el que juzgarán a los auditores en el momento y tal vez pasado el tiempo.

La obsesión de los auditados durante todo el proceso de auditoría habrá sido tener un informe positivo lo que puede traducirse en evitación de conflictos y tal vez en reconocimiento y recompensa.

La obsesión para el auditor ha de ser producir un informe objetivo, veraz y útil que suponga una aportación a la entidad.

El hecho de incluir algunos puntos positivos denota que el informe no es exclusivamente una relación de puntos negros, y anima a los auditados. No está de más incluir algún párrafo aclarando que el informe se refiere, a los puntos susceptibles de mejora o de un mayor control, obviando los que están dentro de la normalidad.

Otros aspectos a tener en cuenta son: el informe debe estar fechado, convenientemente firmado en todas sus hojas, el número de página respecto a las totales, el número de copia, el destinatario del mismo, y otros datos que ayuden a identificar de donde ha procedido la filtración de dicho informe en caso de producirse.

Estructura del informe

- **Introducción**

- Índice: No es necesario si el informe tiene pocas páginas.
- Antecedentes
- Objetivo y ámbito de la auditoría: A veces el objetivo principal de la auditoría no se manifiesta a los auditores, o bien se dice pero no debe especificarse en los informes.
- Agradecimientos: Pueden referirse a las facilidades que ha habido, a la documentación recibida, a los entrevistados por su tiempo dedicado...
- Descripción del entorno informático: Puede comenzar por alguna referencia a la entidad, a su posicionamiento en el mercado, al sector, al grupo de entidades... si ello puede tener relación con la situación de la informática y su valoración: riesgos específicos del sector, crisis que pueda relacionarse con tecnología obsoleta, limitaciones presupuestarias, convenios con incrementos limitados...
- Limitaciones: pueden ser totales (la auditoría no se puede finalizar) o parciales que es lo habitual:
 - Documentación solicitada a la que no se ha llegado a tener acceso
 - Personas a las que no se ha podido entrevistar
 - Instalaciones que no se han visitado
 - El periodo al que se han referido algunas comprobaciones
 - Dificultades por la complejidad del entorno
- Diagnóstico-resumen

- **Cuerpo**

Algunos auditores estructuran el informe por tipos de control, pero en la práctica suele ser preferible estructurarlo por áreas, pudiéndose realizar desgloses por grupos en el caso de instalaciones complejas; de este modo se facilita la discusión con auditados y la distribución y seguimiento de puntos responsables de la entidad.

En cada punto (o grupo de puntos) debe incluir:

- Descripción de la deficiencia con precisión
- Causa
- Efecto (importancia y riesgo)
- Recomendación: Debe ser viable y que no sea absolutamente prohibitiva en cuanto a coste para el tipo de instalación.

Dentro del informe los auditores deben asignar prioridades en función del riesgo.

- **Anexos**

Pueden no existir, en este apartado se incluirá la información que no debe interferir ni engordar el cuerpo del informe, alguna información a incluir:

- Entrevistas/contactos
- Algunos cuestionarios usados y resultados
- Documentación utilizada
- Gráficos
- Listados: si se incluyen no deben ser voluminosos y solo si son imprescindibles para demostrar algo importante.

Proceso del borrador

Debe realizarse una revisión del borrador del informe, además de por parte del gerente o jefe de auditoría por personas ajenas al proceso.

No puede considerarse más que un borrador, ya que ha de entregarse a los auditados para que lo lean y mantener después una reunión.

En esta reunión deben aclararse totalmente todos los puntos y aportar evidencias tanto auditados como auditores hasta llegar a acuerdos sin que los auditores cedan en sus opiniones si no se les demuestra fehacientemente que estaban equivocados.

A veces se admite algún cambio de palabras o de frases a sugerencia de los auditados si con ello no se ve afectada la esencia de los puntos indicados.

Informe definitivo

La entrega del informe propiamente dicho se hará:

- En el caso de auditores internos a quien esté establecido según las normas de la entidad.
- En el caso de los externos a quien haya encargado la auditoría.

Y en todo caso, si existe un Comité de Auditoría, se le debe entregar una copia; de no existir, y si esa es la norma de la entidad, se le puede entregar al Comité de Informática o de Sistemas de Información.

Respecto a las acciones a iniciar, la entidad debe decidir sobre qué hacer respecto a las debilidades y aspectos mejorables señalados por el informe.

Capítulo 7

Sistemas de Gestión de Seguridad de la Información (SGSI)

ISO / IEC 27001

7.1 Definición de SGSI

Un Sistema de Gestión de Seguridad de la Información o SGSI, también conocido como ISMS por sus siglas en inglés (*Information Security Management System*) se puede definir como un conjunto de políticas de administración de la información.

En una definición más amplia, el SGSI incluye tanto la organización como las políticas, la planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Es decir, tanto la documentación de soporte como las tareas que se realizan.¹⁴

Es un término utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término.

¹⁴ Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes
http://www.aenor.es/aenor/descargadocumento.asp?nomfich=/Documentos/Comercial/Archivos/NOV_DOC_Tabla_AEN_22994_1.pdf&cd_novedad=&cd_novedad_doc=1

7.2 Ciclo de mejora continua

Para gestionar un SGSI se utiliza un ciclo PDCA de mejora continua, también conocido como ciclo de Deaming.

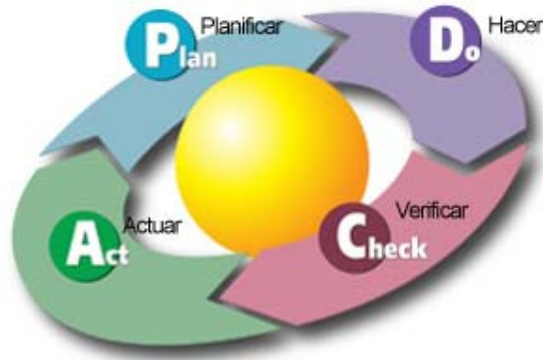


Figura 36. Ciclo PDCA

Es la metodología más usada para implantar un sistema de mejora continua.

El ciclo PDCA, siglas en inglés de *Plan*, *Do*, *Check*, *Act*, o “Planificar, Hacer, Verificar, Actuar”, se divide en las cuatro fases¹⁵ que indica su nombre:

- **Planificar (Plan):** es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- **Hacer (Do):** envuelve la implantación y operación de los controles.
- **Verificar (Check):** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Actuar (Act):** en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

¹⁵ http://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n

7.3 Norma ISO / IEC 27001

7.3.1 Definición

ISO / IEC 27001 es un estándar internacional de referencia para la seguridad de la información.

Especifica los requisitos para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). En definitiva, define cómo se debe gestionar la seguridad de la información en una empresa.

Se basa en el ciclo de vida PDCA que vimos en el apartado anterior.

La última versión fue publicada en el año 2013, y se denomina ISO/IEC 27001:2013.



Figura 37. ISO / IEC 27001:2013

7.3.2 Estructura

Se divide en 11 secciones, a su vez agrupadas como introductorias u obligatorias, además de un anexo.

- **Secciones introductorias:** No son obligatorias para la implementación.
 - ✓ **Sección 0. Introducción.** Explica el objetivo de la norma, así como su compatibilidad con otras normas existentes de gestión.
 - ✓ **Sección 1. Alcance.** Explica que esta norma es aplicable a cualquier tipo de organización.
 - ✓ **Sección 2. Referencias normativas.** Recomienda la consulta de algunos documentos indispensables para la aplicación de la norma.
 - ✓ **Sección 3. Términos y definiciones.**
- **Secciones obligatorias:** Para cumplir con la norma se deben implementar todas y cada una de las siguientes secciones.
 - ✓ **Sección 4. Contexto de la organización.** Define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
 - ✓ **Sección 5. Liderazgo.** Define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
 - ✓ **Sección 6. Planificación.** Define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

- ✓ **Sección 7. Soporte.** Define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- ✓ **Sección 8. Operación.** Define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
- ✓ **Sección 9. Evaluación de desempeño.** Define los requerimientos de monitorización, medición, análisis, auditoría interna y revisión por parte de la dirección.
- ✓ **Sección 10. Mejora.** Define los requerimientos para tratar las deficiencias encontradas, aplicación de medidas correctivas y mejora continua.
- **Anexos:** Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.
 - ✓ **Anexo A** – Proporciona un catálogo de 113 controles (medidas de seguridad) distribuidos en 14 dominios (A.5 a A.18).

A continuación se muestra la distribución de las secciones en el ciclo PDCA.

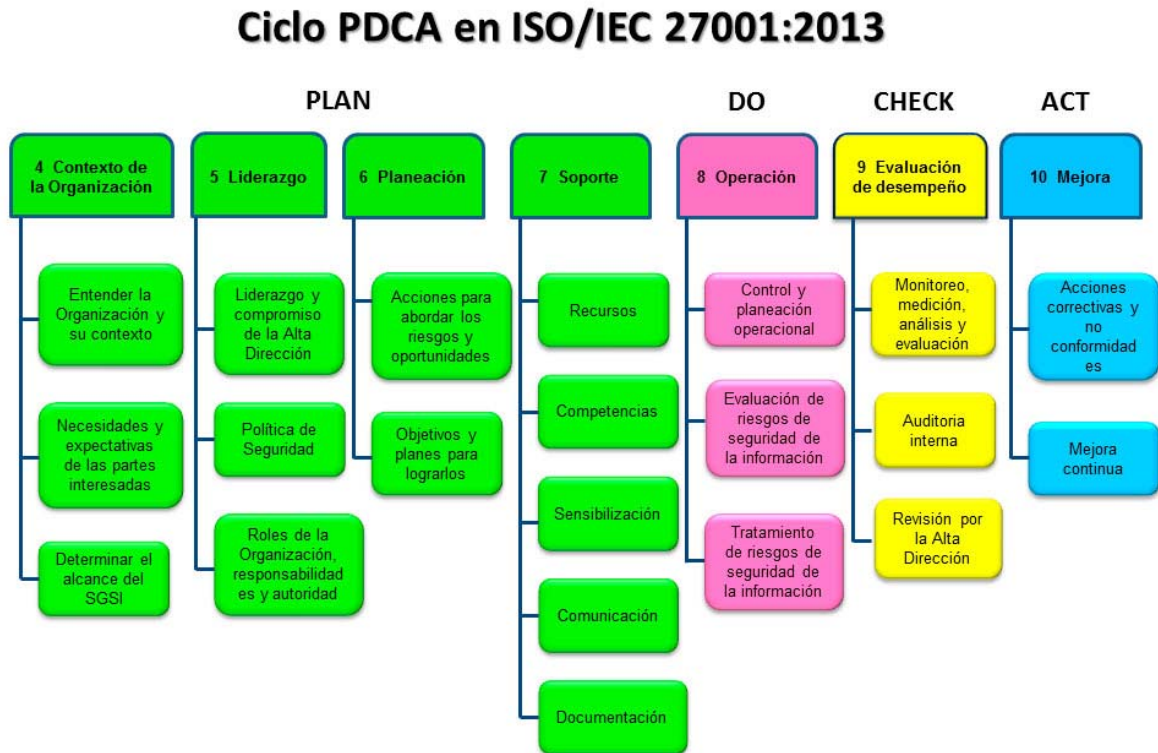


Figura 38. Ciclo PDCA en ISO/ IEC 27001:2013

7.3.3 Implementación

Para implementar la norma ISO 27001, es recomendable seguir los siguientes pasos:

1) Obtener el apoyo de la dirección

Uno de los principales escollos que se encuentra en la implementación de la norma es no haber obtenido desde un primer momento el suficiente apoyo de la dirección de la organización.

Por tanto, es importante que la dirección, comprenda y esté concienciada de los beneficios que obtendrá de la implementación de la norma, así como la amortización de los recursos personales y económicos empleados.

Se pueden argumentar una serie de grandes beneficios de la implementación de la norma:

a. Activo de comercialización

El cumplimiento de la norma puede ser un valor añadido de la organización, resultando un punto atractivo para los clientes y de diferenciación con la competencia.

b. Reducción de gastos

A priori se puede pensar que los recursos económicos invertidos en la seguridad de la información no producen un retorno económico. Sin embargo, se debe contabilizar una ganancia si se consiguen disminuir los gastos generados por incidencias, indisponibilidades, o falta de efectividad en algunas tareas que afecten directamente al rendimiento de la organización.

c. Orden en la estructura de la organización

La implantación de la norma obliga a definir de forma precisa los roles y responsabilidades de cada puesto o empleado. De esta forma, la empresa

tendrá una estructura ordenada, teniendo claro quién debe hacer qué y hasta donde llega la responsabilidad de cada uno. Esto puede ayudar a optimizar el trabajo de día a día de la empresa, así como a dimensionar los recursos humanos necesarios.

2) Utilizar una metodología para gestión de proyectos

La implementación de la norma ISO 27001 no es trivial, se compone de muchas fases y actividades, involucra a muchas personas y puede alargarse en el tiempo requiriendo varios meses o incluso más de un año.

Al ser un tema tan complejo, para que el trabajo llegue a buen puerto, debe definirse claramente qué es lo que se hará, quién lo hará y en qué momento.

3) Definir el alcance

Sobre todo en organizaciones grandes es muy importante definir el alcance de la implementación. Si la organización es demasiado grande, y se pretende abarcar demasiado, los riesgos para finalizar la implementación pueden ser demasiado elevados.

4) Redactar una política de alto nivel sobre seguridad de la información

La política de seguridad de la información es el documento con mayor importancia en el SGSI.

Debe contemplar, a un alto nivel, aspectos básicos sobre la seguridad de la información.

Su principal objetivo es que la dirección defina claramente qué aspectos desea conseguir y cómo llegar a controlarlos.

5) Definir la metodología de evaluación de riesgos

La evaluación de riesgos es considerada la tarea más compleja. El objetivo es definir las reglas para identificar los activos, las vulnerabilidades, las

amenazas, las consecuencias y las probabilidades, así como definir el nivel aceptable de riesgo.

Si esas reglas no están bien definidas, los resultados de la implementación pueden resultar inútiles o insatisfactorios.

6) Realizar la evaluación y el tratamiento de riesgos

Se debe realizar la implementación de lo definido en el paso anterior.

El objetivo es identificar y reducir los riesgos definidos como no aceptables. Para ello es aconsejable el uso de los controles definidos en el Anexo A de la norma.

Como documento de salida, se redacta un Informe sobre la evaluación de riesgos que contendrá todas las acciones tomadas durante el proceso.

7) Redactar la Declaración de aplicabilidad

Una vez realizada la evaluación y el tratamiento de riesgos, se conocerán qué controles del Anexo son aplicables a la organización. Con estos datos, se generará un documento con la siguiente información:

- Enumeración de todos los controles.
- Identificación de cuáles son aplicables y cuáles no, incluyendo los motivos de esa decisión.
- Descripción de los objetivos que se lograrán.
- Explicación de cómo se implementarán.

8) Redactar el Plan de tratamiento de riesgos

El objetivo del documento es definir cómo, quién, cuándo y con qué recursos se implementarán los controles de la Declaración de aplicabilidad.

Por lo tanto, es el detalle del plan de implementación de los controles, a partir del cual se abordarán los siguientes pasos.

9) Definir la forma de medir la eficacia de los controles

Uno de los principales escollos que nos podemos encontrar es como saber si hemos logrado el objetivo de los controles establecidos. Para ello es muy importante establecer un criterio de medida cuantitativo del logro de los objetivos, tanto a nivel global como en cada control realizado.

10) Implementar todos los controles y procedimientos necesarios

Es la fase crítica del proyecto, hay que poner en práctica la implantación de las metodologías. Esto conlleva tareas que pueden parecer triviales pero resultan muy complicadas, como son la aplicación de nuevas tecnologías, asignación de nuevas tareas o funciones al personal laboral, etc.

11) Implementar programas de capacitación y concienciación

Para que los empleados cumplan adecuadamente con las nuevas medidas implantadas es muy importante que entiendan el origen del problema, por qué se implantan esas nuevas políticas, y además hayan recibido la formación adecuada para saber cómo actuar en las diferentes situaciones que se planteen.

12) Realizar todas las operaciones diarias establecidas en la documentación de su SGSI

Deben registrarse las operaciones diarias relativas a los controles y procedimientos implantados en la organización.

Con estos registros resultará más fácil hacer un seguimiento de las tareas realizadas y, en caso de encontrar nuevas disconformidades, encontrar la causa que las ha provocado.

13) Monitorear y medir su SGSI

En este punto se debe comprobar, utilizando la metodología de medición adoptada, si los resultados que se obtienen cumplen con los objetivos que se han establecido.

En caso contrario, se deben aplicar nuevas medidas correctivas para subsanarlo.

14) Realizar la auditoría interna

La gran mayoría de las deficiencias o “no conformidades” que se encuentran se deben a que las personas que las cometen no son conscientes de que lo están haciendo, o por el contrario, lo saben pero lo encubren para no ser descubiertos.

Una auditoría interna puede despejar estas situaciones, haciendo ver a los empleados que no se quieren tomar medidas disciplinarias contra las personas, sino que el objetivo es atacar los problemas aplicando medidas preventivas y correctivas.

15) Realizar la revisión por parte de la dirección

La dirección no debe entrar a en detalles técnicos, pero sí debe conocer en todo momento el estado de la implantación del SGSI. Ya que debe tomar decisiones en función de algunos aspectos importantes, como si se están obteniendo los resultados deseados o si los recursos asignados están cumpliendo con su cometido entre otros.

16) Implementar medidas correctivas y preventivas

El principal objetivo del SGSI es subsanar las “no conformidades” detectadas durante el proceso. Para ello se deben implementar medidas concretas y sistemáticas para cada una de las deficiencias encontradas.

Las medidas se deben enfocar actuando sobre dos puntos: corrección y prevención. Como hemos dicho, lo principal es corregir las deficiencias

encontradas, pero una vez subsanadas, es más importante aún, y siempre que sea posible, tomar las medidas necesarias que las prevengan.

7.3.4 Certificación

La norma ISO 27001 es certificable. Lo que permite que una empresa, y en concreto su SGSI, sea auditado por una entidad de certificación acreditada e independiente. Y así, una vez superada la auditoría, obtener la certificación que confirma que la seguridad de la información de la organización ha sido implementada cumpliendo los requisitos de la norma.

Evidentemente, la implantación de un SGSI en una empresa no obliga a certificarse en la norma. Sin embargo, obtener dicha certificación es factor muy importante de cara al público y los mercados para demostrar que la empresa es confiable y se gestiona de forma clara y transparente.

Por este motivo, el número de empresas que han decidido certificarse en la norma ha aumentado considerablemente en los últimos años.

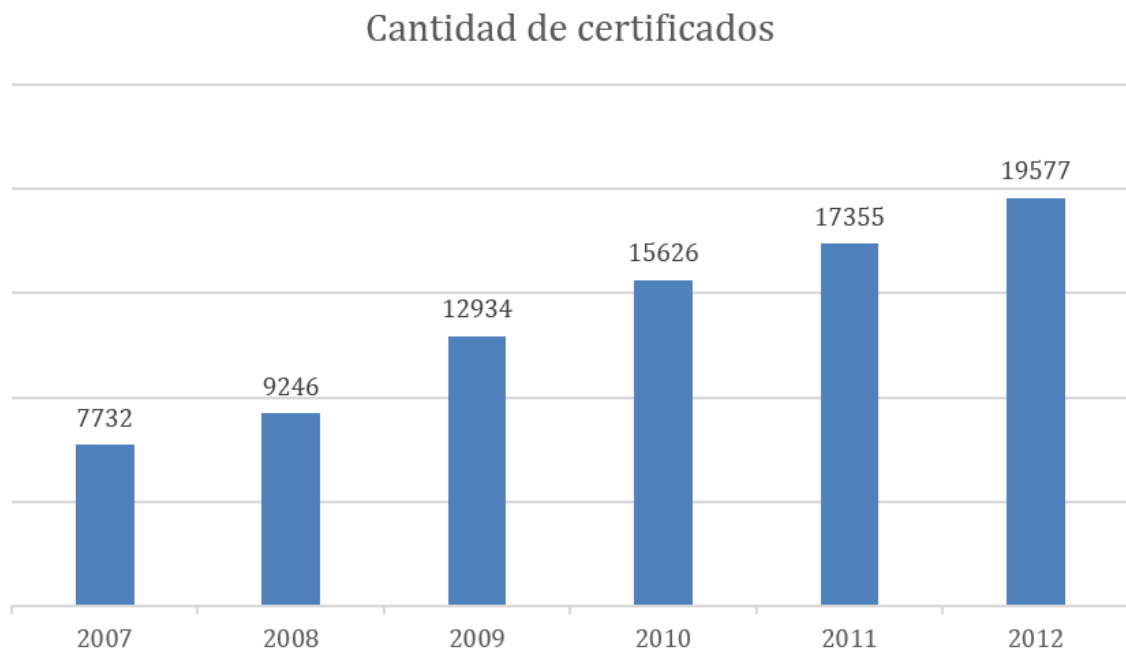


Figura 39. Ciclo PDCA en ISO/ IEC 27001:2013

7.3.5 Anexo A

ISO 27001:2013 Anexo	Sección
A.5 Políticas de Seguridad de la Información	
A.5.1	Dirección de gestión de Seguridad de la Información
A.5.1.1	Documentos de la Política de la Seguridad de la Información
A.5.1.2	Revisión de las políticas de Seguridad de la Información
A.6 Organización de la Seguridad de la Información	
A.6.1	Organización Interna
A.6.1.1	Los roles de Seguridad de la Información y las responsabilidades
A.6.1.2	Segregación de funciones
A.6.1.3	Contacto con las autoridades
A.6.1.4	Contacto con grupos de especial interés
A.6.1.5	Seguridad de la Información en la gestión de proyectos
A.6.2	Los dispositivos móviles y el teletrabajo
A.6.2.1	Política de dispositivo móvil
A.6.2.2	Teletrabajo
A.7 Seguridad de los recursos humanos	
A.7.1	Antes del empleo
A.7.1.1	Selección
A.7.1.2	Términos y condiciones de contratación
A.7.2	Durante el empleo
A.7.2.1	Responsabilidades de la dirección
A.7.2.2	Concienciación, formación y capacitación en SI
A.7.2.3	Proceso disciplinario
A.7.3	Término y cambio de empleo
A.7.3.1	Responsabilidad en termino y cambio de empleo
A.8 Gestión de activos	
A.8.1	Responsabilidad sobre los activos
A.8.1.1	Inventario de activos
A.8.1.2	Propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devolución de activos
A.8.2	Clasificación de la información
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A.8.2.3	Manejo de activos
A.8.3	Manejo de los medios de información
A.8.3.1	Gestión de medios removibles

A.8.3.2	Retiro de los medios de información
A.8.3.3	Transferencia física de los medios de información
A.9 Control de acceso	
A.9.1	Requisitos del negocio para el control de acceso
A.9.1.1	Política de control de acceso
A.9.1.2	El acceso a redes y servicios de red
A.9.2	Gestión de acceso de usuario
A.9.2.1	Registro de usuario
A.9.2.2	Entrega de acceso de usuario
A.9.2.3	Gestión de privilegios
A.9.2.4	Gestión de contraseña de usuarios
A.9.2.5	Revisión de los derechos de acceso de usuario
A.9.2.6	Eliminación o ajuste de derechos de acceso
A.9.3	Responsabilidades del usuario
A.9.3.1	El uso de contraseña
9.4	Sistema de control de acceso a la aplicación
9.4.1	Restricción de acceso a la información
9.4.2	Procedimientos de inicio de sesión seguros
9.4.3	Sistema de gestión de contraseñas
9.4.4	Uso de programas con privilegios
9.4.5	Control de acceso al código fuente
10 Criptografía	
A.10.1	Controles criptográficos
A.10.1.1	Política de uso de los controles criptográficos
A.10.1.2	Gestión de claves
11 Seguridad física y ambiental	
A.11.1	Áreas seguras
A.11.1.1	Perímetro de seguridad física
A.11.1.2	Controles de entrada físicas
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones
A.11.1.4	Protección contra amenazas externas y ambientales
A.11.1.5	Trabajar en zonas seguras
A.11.1.6	Áreas de acceso al público de carga y descarga
A.11.2	Equipo
A.11.2.1	Ubicación y protección del equipo
A.11.2.2	Servicios de apoyo
A.11.2.3	Seguridad Cableado
A.11.2.4	Mantenimiento de los equipos
A.11.2.5	Eliminación de los activos
A.11.2.6	Seguridad de los equipos fuera de las instalaciones
A.11.2.7	Eliminación segura o re - uso de equipos
A.11.2.8	Equipo de usuario desatendida
A.11.2.9	Políticas de escritorios y pantallas limpias

A.12 Operaciones de seguridad	
A.12.1	Procedimientos y responsabilidades operacionales
A.12.1.1	Documentos de los procedimientos de operación
A.12.1.2	Gestión de cambios
A.12.1.3	Gestión de la capacidad
A.12.1.4	Separación de los entornos de desarrollo, prueba y operación
A.12.2	Protección contra malware
A.12.2.1	Controles contra el malware
A.12.3	Backup
A.12.3.1	Copias de seguridad de la información
A.12.4	Registro y control
A.12.4.1	Registro de auditorías
A.12.4.2	Protección de los LOG de información
A.12.4.3	Administración y operación de LOG
A.12.4.4	Sincronización horaria
A.12.5	Control de software operativo
A.12.A.5.1	Instalación del software en los sistemas operativos
A.12.6	Gestión de vulnerabilidades técnicas
A.12.A.6.1	Gestión de las vulnerabilidades técnicas
A.12.A.6.2	Restricciones en la instalación de software
A.12.7	SI consideraciones de auditoría
A.12.A.7.1	Controla Información auditoría de sistemas
A.13 Seguridad de las comunicaciones	
A.13.1	Gestión de la seguridad de red
A.13.1.1	Controles de red
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Segregación en las redes
A.13.2	Transferencia de información
A.13.2.1	Políticas y los procedimientos de transferencia de información
A.13.2.2	Los acuerdos sobre la transferencia de información
A.13.2.3	Mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o de no divulgación
A.14 Sistema de adquisición, desarrollo y mantenimiento	
A.14.1	Requisitos de seguridad de sistemas de información
A.14.1.1	SI de análisis de requisitos y especificaciones
A.14.1.2	Protección de servicios de aplicaciones en redes públicas
A.14.1.3	Protección de las transacciones de servicios de aplicaciones
A.14.2	Seguridad en los procesos de desarrollo y soporte
A.14.2.1	Política de desarrollo seguro
A.14.2.2	Procedimientos de control de cambios
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios
A.14.2.4	Restricciones a los cambios en los paquetes de software
A.14.2.5	Principios de ingeniería de seguridad de sistemas

A.14.2.6	Entorno de desarrollo seguro
A.14.2.7	Externalización de desarrollo de software (Outsourced)
A.14.2.8	Pruebas de seguridad del sistema
A.14.2.9	Pruebas de aceptación del sistema
A.14.3	Datos de prueba
A.14.3.1	Protección de los datos de prueba
A.15 Relaciones con los proveedores	
A.15.1	SI en relación con los proveedores
A.15.1.1	Política de SI de los proveedores
A.15.1.2	Abordar la SI dentro de acuerdos con proveedores
A.15.1.3	Información y cadena del suministro de la tecnología de la comunicación
A.15.2	Gestión de la prestación de servicios de proveedor
A.15.2.1	Monitoreo y revisión de los servicios de proveedores
A.15.2.2	Gestión de cambios en los servicios de proveedores
A.16 Gestión de incidentes de SI	
A.16.1	Gestión de los incidentes de SI y mejoras
A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Eventos de seguridad informática
A.16.1.3	Información debilidades de SI
A.16.1.4	Evaluación y decisión sobre los eventos de SI
A.16.1.5	Respuesta a incidentes de SI
A.16.1.6	Aprendiendo de los incidentes de SI
A.16.1.7	Reunión de pruebas
A.17 Aspectos de SI de gestión de la PC	
A.17.1	Información de la continuidad de seguridad
A.17.1.1	Planificación de la continuidad de la SI
A.17.1.2	Implementación de continuidad SI
A.17.1.3	Verificar , revisar y evaluar la continuidad de SI
A.17.2	Despidos
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información
A.18 Cumplimiento	
A.18.1	Cumplimiento de los requisitos legales y contractuales
A.18.1.1	Identificación de la legislación aplicable y requisitos contractuales
A.18.1.2	Derechos de propiedad intelectual
A.18.1.3	Protección de los registros
A.18.1.4	Privacidad y protección de datos personales
A.18.1.5	Regulación de controles criptográficos
A.18.2	Opiniones seguridad de la información
A.18.2.1	Revisión independiente de la seguridad de la información
A.18.2.2	Cumplimiento de las políticas y normas de seguridad
A.18.2.3	Revisión de cumplimiento técnico

Capítulo 8

Conclusiones

8.1 Conclusiones personales

8.1.1 Experiencias alcanzadas

La realización de este Proyecto me ha servido para ampliar mis conocimientos sobre el mundo de redes inalámbricas, los cuales antes de empezar este trabajo iban poco más allá de saber configurar una red doméstica.

Sin embargo, tras la realización del mismo, mis conocimientos se han ampliado a la existencia de los diferentes estándares, las posibilidades de cada uno, así como sus fortalezas y vulnerabilidades.

También considero que he adquirido suficientes conocimientos para poder detectar deficiencias de seguridad en una red inalámbrica, y además, realizar una serie de recomendaciones para subsanarlas.

Por último, el desarrollo del prototipo en un entorno tecnológico tan actual como Android, me ha servido para aprender un nuevo lenguaje de programación, y ayudado a conocer sus posibilidades y potencial para futuros usos.

8.1.2 Objetivos cumplidos

Al principio de este trabajo se fijaban una serie de objetivos principales y secundarios. Una vez finalizado el mismo, considero que se han cubierto todos ellos, tanto los propios como autor del proyecto como los del trabajo en sí mismo.

8.1.3 Contribución

Con este trabajo se aporta una introducción lo más sencilla y concisa posible al mundo de lo inalámbrico. Para que cualquier persona, basándose en el estudio teórico, adquiera una base de conocimiento sobre el entorno inalámbrico, así como de la necesidad de las auditorías y normas aplicables.

Se realizan una serie de recomendaciones esenciales y fáciles de poner en práctica, ya sea en un entorno laboral o doméstico, con las cuales el riesgo de sufrir un ataque o intromisión se reduce considerablemente.

La herramienta desarrollada en Android elimina la necesidad de llevar consigo el Excel o papeles con el *check list* de apoyo. Pudiendo ejecutar la aplicación en cualquier momento y lugar fácilmente desde nuestro *smartphone* para comprobar la seguridad de una red, obteniendo además de manera dinámica las recomendaciones oportunas en función de las respuestas aportadas.

8.1.4 Líneas de futuro

Este trabajo puede ser un punto de partida para la ampliación de la parte teórica según van evolucionando las redes inalámbricas, así como para futuros estudios sobre aplicaciones de normas para la seguridad de las redes.

A su vez, las recomendaciones mostradas, y el *check list* de apoyo pueden ser utilizados para trabajos más amplios de auditoría.

También la aplicación desarrollada para Android pudiera ser un buen punto de partida como herramienta con utilidades indispensables para realizar auditorías a redes inalámbricas.

8.2 Recomendaciones de seguridad

Como hemos visto a lo largo de este trabajo, mientras que para poder atacar en redes cableadas es necesario conectarse físicamente mediante un cable, en las redes inalámbricas se convierte en una tarea mucho más sencilla.

No solo existen los mismos peligros que ya teníamos en las redes cableadas, sino que además se suman nuevos puntos débiles.

Los protocolos 802.11 implementan una serie de mecanismos de cifrado para proteger nuestros datos que viajan por el aire, la gran mayoría de las veces mucho más allá de las paredes de nuestra casa y/u organización.

Pero de la misma forma hemos visto que muchos de ellos tienen sus puntos débiles, ya sea por debilidad propia del mecanismo o por falta de administración del mismo, por lo que no podemos considerar que estamos seguros por el mero hecho de tener un cifrado de datos.

Lo ideal para mantener nuestra red protegida e incluso oculta es tener en cuenta una serie de recomendaciones a seguir para mejorar la seguridad de nuestra red:

- **Asegurar el punto de acceso**
 - **Controlar el acceso físico al punto de acceso**

El punto de acceso es la puerta de entrada a la red inalámbrica, por lo tanto debe estar protegido igualmente ante la manipulación física por parte de cualquier persona.

Debe ubicarse en lugares donde solo tengan acceso los administradores de los mismos. Si estuviese accesible para cualquier persona, es

susceptible de conectarse a la red físicamente mediante cable o bien de manipularlo para afectar su correcto funcionamiento.

- **Controlar el alcance de la red**

La mayoría de los puntos de acceso permiten ajustar la fuerza de la señal, y por lo tanto su alcance efectivo.

Es importante estudiar bien la ubicación de los puntos de acceso, colocándolos lo más alejados posibles de paredes y ventanas exteriores.

- **Cambiar la contraseña por defecto**

Habitualmente, los fabricantes siempre establecen la misma contraseña por defecto para acceder a la administración del punto de acceso.

Esto hace que si los administradores no la modifican, como en muchas ocasiones ocurre, cualquier persona pueda acceder a la administración de dichos puntos de acceso.

A la hora de elegir la contraseña, es importante evitar las que sean fáciles de deducir, como fecha de nacimiento o nombre de mascota. Además para evitar ataques de diccionario, evitar palabras comunes, y usar contraseñas que contengan letras, números y caracteres especiales.

- **Seguridad de los datos transmitidos**

- **Cifrado wifi**

Aplicando protocolos de seguridad con cifrado conseguiremos proteger los datos en la comunicación, tanto para el acceso a la red, como para la información intercambiada. Por lo que aunque pudieran ser escuchados, en teoría nadie que no conozca la clave puede interpretarlos.

Como hemos visto, existen diferentes protocolos que permiten el cifrado, por lo que es importante saber cuál se debe elegir a la hora de configurar nuestra red.

Se debería elegir alguna de las siguientes alternativas, ordenadas por orden de preferencia de mayor a menos seguridad:

- **WPA2 (Wifi Protected Access 2):** Hasta el momento se considera la opción más segura.

Existen dos posibilidades para la autenticación:

- **WPA2-Enterprise:** Sin duda la mejor opción. Sin embargo es más costosa, ya que requiere de una infraestructura de autenticación 802.1x con un servidor de autenticación, normalmente un servidor RADIUS.
- **WPA2-Personal:** No necesita servidor de autenticación. La autenticación se hace mediante una clave precompartida (PSK) entre los dispositivos que van a autenticarse mutuamente.

Además implementa dos opciones con algoritmos de cifrado diferentes para los datos:

- **AES:** Algoritmo más seguro.
 - **TKIP:** Se utiliza para mantener compatibilidad con los dispositivos WPA.
- **WPA (Wifi Protected Access):** trataba de corregir las vulnerabilidades conocidas del protocolo WEP. Al igual que WPA2 ofrece dos posibles configuraciones, la única diferencia es que WPA no dispone del algoritmo AES.
 - **WEP (Wired Equivalent Protocol):** Es fácilmente descifrable, hoy en día cualquier atacante puede romperlo en poco tiempo.

En ocasiones se sigue utilizando por compatibilidad con otros dispositivos antiguos que necesitan conectar a la red.

En caso de tener que utilizarla, al menos usar claves de 128 bits y no de 64.

NONE: No existe cifrado, cualquier usuario se podrá conectar a la red, no solo para utilizar tu acceso a internet, sino también a tus dispositivos conectados a la red. Además cualquier uso indebido de internet por parte del atacante, podrá ser achacado al propietario de la conexión a internet.

- **Elección de la clave**

Habitualmente este tipo de contraseñas admite más de 60 caracteres, y como ya hemos visto la longitud y complejidad de la misma es importante ante un ataque de fuerza bruta o diccionario.

Por lo tanto es recomendable utilizar claves largas, utilizando letras (tanto mayúsculas como minúsculas), números y caracteres especiales.

También se recomienda modificar la clave periódicamente, evitando repetirla de nuevo en cortos periodos de tiempo.

- **Ocultar la red**

- **Cambiar el SSID por defecto**

Al igual que ocurre con las contraseñas, los fabricantes o los proveedores de internet en caso de equipos facilitados por estos, asignan SSID por defecto a los puntos de acceso.

Es recomendable modificar esos nombres para evitar dar información sobre el hardware utilizado, y por tanto sus debilidades si las tuviera, a los posibles atacantes.

A la hora de elegir el nombre de la red, lo recomendable es no utilizar nada descriptivo, como nombre de la empresa o personas. Es mejor utilizar nombres que no llamen la atención y pasen desapercibidos entre otras redes.

- **Desactivar la difusión del SSID**

Difundir el SSID facilita que los nuevos clientes que desean conectar a la red identifiquen automáticamente los datos de esta. Pero de la misma manera, permite a cualquiera dentro del alcance identificar la red, su nombre, su cobertura e incluso el protocolo de seguridad utilizado.

Si se desactiva esta opción, el cliente debe introducir manualmente el nombre de la red, por lo tanto ha de conocer la existencia de ella y su nombre de antemano.

- **Evitar que se conecten**

- **Activar el filtrado de direcciones MAC**

Es recomendable activar en el punto de acceso el filtrado de direcciones MAC. Para ello se introduce el listado de direcciones MAC de los dispositivos cliente que habitualmente están conectados a la red, de esta forma se denegará la conexión a cualquier dispositivo cuya MAC no se encuentre en dicho listado.

- **Establecer el número máximo de dispositivos que pueden conectarse**

Habitualmente se puede configurar en los puntos de acceso el número máximo de dispositivos que pueden conectarse al mismo tiempo. De esta manera, si es una red más o menos fija, se consigue que se deniegue cualquier intento de conexión más allá de ese número de dispositivos.

- **Desactivar DHCP**

De esta forma se obliga a configurar manualmente ciertos parámetros en los equipos cliente que desean conectarse. Por lo que se han de conocer de antemano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

- **Medidas adicionales**

- **Apagar el punto de acceso cuando no se utilice**

Siempre que la actividad lo permita, una buena práctica es apagar el punto de acceso cuando no se esté usando. Por ejemplo, en las oficinas fuera del horario laboral o en fines de semana.

De esta forma se elimina, durante ese periodo de tiempo, el único punto mediante el cual un atacante puede acceder a la red.

8.3 Check list de apoyo para la seguridad inalámbrica

Considerando los puntos reflejados en las conclusiones, he generado una check list de apoyo para auditar redes WIFI:

	Cuestiones a auditar	Si/No	Obs.
Acceso a los puntos de acceso de la red			
1	Los puntos de acceso a la red están actualizados con el último Firmware oficial disponible		
2	Los puntos de acceso a la red están situados en zonas restringidas, siendo tan sólo accesibles por personal autorizado		
3	El acceso remoto a la administración de los puntos de acceso a la red está restringido (solo desde LAN)		
4	La contraseña de administrador de los puntos de acceso es modificada al menos cada 6 meses		
5	La contraseña de administrador es segura. Contiene minúsculas, mayúsculas, números y caracteres especiales		
6	La dirección IP de red local de los puntos de acceso ha sido modificada (no es la de por defecto)		
7	Los servicios, interfaces y protocolos sin uso o que no son estrictamente necesarios están deshabilitados		
8	Se apagan los puntos de acceso a la red si no se va a ser utilizados en periodos de tiempo prolongados		
Acceso a la red			
9	El SSID refleja datos identificativos de la empresa o su actividad		
10	Se propaga el SSID o nombre de la red		
11	La intensidad de la señal se ajusta a los límites físicos de la organización		
12	La red tiene en todo momento habilitado un algoritmo de cifrado		

13	Se utiliza el algoritmo de cifrado WPA-PSK o WPA2/PSK		
14	Los puntos de acceso tienen la opción de filtrado por MAC habilitada		
15	Los administradores de red mantienen un listado con la MAC de todos los equipos cliente de la red		
16	Se define en los puntos de acceso a la red un número máximo de dispositivos que pueden conectar a ellos		
17	Los puntos de acceso a la red tienen el servicio WPS deshabilitado		
18	Los puntos de acceso a la red tienen el servicio DHCP deshabilitado		
Políticas de contraseñas			
19	La contraseña de acceso a la red es segura. Contiene minúsculas, mayúsculas, números y caracteres especiales		
20	Las contraseñas son modificadas al menos cada 6 meses		
21	Existen políticas de comunicación de contraseña adecuadas		
Equipos cliente			
22	Los usuarios de la red tienen apuntadas las contraseñas en lugares visibles o en ficheros en claro almacenados en el ordenador		
23	Los equipos cliente de la red se actualizan con los parches de seguridad recomendados		
24	Los equipos cliente de la red tienen antivirus instalados y son actualizados periódicamente		
25	Los equipos cliente de la red tienen los firewall personales habilitados		
26	Los equipos cliente de la red tienen contraseña para el inicio de sesión		
27	Modo ad-hoc está deshabilitado en todos los equipos		
Políticas de revisión de logs			
28	Existe política de revisión de logs de acceso en los puntos de acceso a la red		

Capítulo 9

Prototipo de aplicación

9.1 Análisis

9.1.1 Definición del sistema

El prototipo consiste en una aplicación con una interfaz amigable y de uso sencillo cuyos principales objetivos son:

- Poner a disposición del usuario el *check list* de apoyo para seguridad inalámbrica. Se ha elegido el formato cuestionario con el fin de presentarlo a usuario de un modo intuitivo y sencillo.
- Proporcionar dentro de la propia aplicación las herramientas necesarias para poder completar el *check list* sin necesidad de herramientas externas adicionales.
- Convertirse en una herramienta útil para determinar en unos pocos pasos si una red inalámbrica es o no segura.
- Concienciar al usuario sobre la importancia de mantener una seguridad de redes inalámbricas adecuada.

9.1.2 Identificación del entorno tecnológico

Se han analizado diferentes tecnologías actuales teniendo en cuenta las necesidades y objetivos del prototipo. Habiendo considerado como más idóneas las siguientes:

9.1.2.1 Entorno tecnológico del usuario final

Hardware	Dispositivo Móvil de gama baja
SO	Android

Tabla 1. Entorno tecnológico del usuario final

Se ha realizado esa elección pensando en varios puntos:

- **Movilidad de la aplicación:** Que pueda ser ejecutada en dispositivos móviles como *smartphones* o *tablets*, teniéndola así “a mano” en cualquier lugar y cualquier momento.
- **Hardware bajo coste:** Requerimiento de Hardware está al alcance de todos los públicos.
- **Amplitud del universo:** Es el sistema operativo más usado en dispositivos móviles en el mercado.
- **Familiaridad y facilidad de uso para usuario final:** Interfaz con el usuario sea amigable y usable por personas que no tengan conocimientos profundos de auditoría o administración de redes inalámbricas.
- **Facilidad de distribución:** Mediante el Google Play es fácilmente distribuible, llegando sin coste al usuario final.

9.1.2.2 Entorno tecnológico del desarrollador

Equipo de desarrollo	Portatil HP ProBook 6460b
SO	Windows 7
IDE	Android Studio
Hardware de pruebas	Dispositivo Móvil de gama baja

Tabla 2. Entorno tecnológico del desarrollador

9.1.3 Requisitos del software

En este apartado se especifican los requisitos de software identificados.

Se han utilizado los siguientes campos para definir los requisitos:

- **Título:** Nombre del requisito.
- **Identificador:** Identificación unívoca del requisito. Se utiliza la siguiente nomenclatura:
 - RSF-XX: Requisito funcional
 - RSU-XX: Requisito de usabilidad
 - RSR-XX: Requisito de rendimiento

Las XX serán números incrementables.

- **Tipo:** Funcional, de rendimiento o usabilidad.
- **Descripción:** Especifica el significado del requisito.
- **Prioridad:** Alta, Media o Baja.

9.1.3.1 Requisitos funcionales

Identificación de usuarios	
Identificador	RSF-01
Tipo	Funcional
Descripción	El sistema podrá ser utilizado por cualquier usuario sin necesidad de realizar una identificación en la aplicación
Prioridad	Alta

Check List	
Identificador	RSF-02
Tipo	Funcional
Descripción	La aplicación pondrá a disposición del usuario un cuestionario para determinar si una red inalámbrica es segura o no.
Prioridad	Alta

Resultado final	
Identificador	RSF-03
Tipo	Funcional
Descripción	Al finalizar el cuestionario, la aplicación mostrará una serie de recomendaciones para las deficiencias encontradas.
Prioridad	Alta

Herramientas de apoyo	
Identificador	RSF-04
Tipo	Funcional
Descripción	La aplicación proporcionará una serie de herramientas de apoyo con el fin de facilitar al usuario la realización del cuestionario sin la necesidad de herramientas adicionales.
Prioridad	Alta

Aplicación debe ser Offline	
Identificador	RSF-05
Tipo	Funcional
Descripción	La aplicación no dependerá en ningún momento de una conexión a servidores externos en internet. Esto permite mayor flexibilidad de uso.
Prioridad	Alta

Aplicación debe ser fácilmente ampliable / modificable	
Identificador	RSF-06
Tipo	Funcional
Descripción	La aplicación será en la medida de lo posible fácilmente modificable y ampliable, sobre todo a nivel de textos, ampliar o reducir el número de preguntas, etc.
Prioridad	Alta

9.1.3.2 Requisitos de usabilidad

Interfaz intuitiva	
Identificador	RSU-01
Tipo	Usabilidad
Descripción	La aplicación será fácilmente usable sin necesidad de conocimientos previos o formación.
Prioridad	Alta

Lenguaje sencillo	
Identificador	RSU-02
Tipo	Usabilidad
Descripción	Se empleará un lenguaje comprensible y sencillo, evitando términos complicados
Prioridad	Alta

SO Android	
Identificador	RSU-03
Tipo	Usabilidad
Descripción	El sistema será accesible de cualquier dispositivo con SO Android
Prioridad	Alta

Ayuda al usuario	
Identificador	RSU-04
Tipo	Usabilidad
Descripción	La aplicación ofrecerá ayuda en cada una de las pantallas.
Prioridad	Media

9.1.3.3 Requisitos de rendimiento

Fluidez de la aplicación	
Identificador	RSR-01
Tipo	Rendimiento
Descripción	La aplicación debe ser ligera, corriendo en hardware de gama baja sin perjudicar la experiencia de usuario.
Prioridad	Alta

Permisos de Android	
Identificador	RSR-02
Tipo	Rendimiento
Descripción	<p>La aplicación requiere los siguientes permisos del SO Android para funcionar correctamente:</p> <ul style="list-style-type: none">• Almacenamiento

	<ul style="list-style-type: none">○ Modificar/eliminar contenidos del almacenamiento USB• Ubicación<ul style="list-style-type: none">○ Ubicación (GPS) detallada• Comunicación por red<ul style="list-style-type: none">○ Acceso a Internet sin limites• Herramientas del sistema<ul style="list-style-type: none">○ Cambiar estado de Wi-Fi
Prioridad	Alta

9.2 Diseño

La aplicación ha sido diseñada para su uso por el público en general, que sin necesidad de tener conocimientos profundos de seguridad inalámbrica puedan determinar si una red es o no segura, y en caso de no serlo, tomar las medidas correctoras que la aplicación les reporta.

9.2.1 Diagrama de navegación

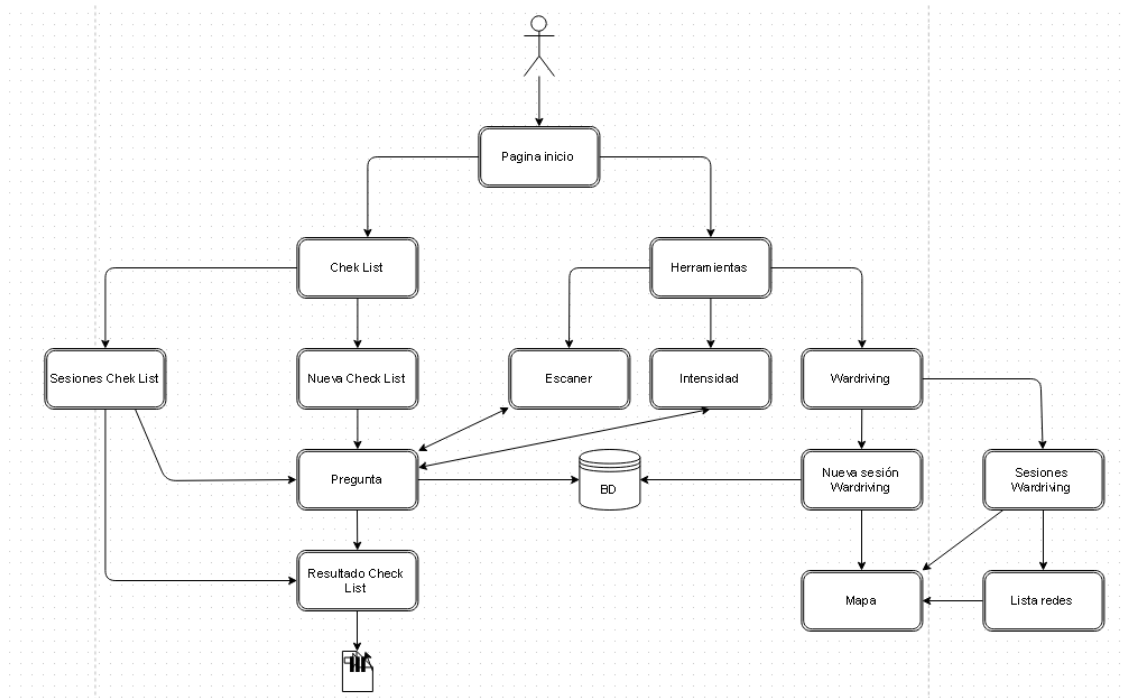


Figura 40. Diagrama de navegación

9.2.2 Estructura de la aplicación

La aplicación se compone de dos bloques diferenciados:

- **Check list de seguridad inalámbrica**

Mediante una serie de preguntas sencillas tipo test dará como resultado un informe con unas recomendaciones sobre puntos débiles o posibles mejoras en la seguridad.

La aplicación está enfocada para poder ser utilizada por cualquier persona, sin necesidad de conocimientos avanzados sobre auditoría o seguridad de redes. Por ello, las preguntas son cortas y sencillas. Además se provee de ayuda y de las herramientas necesarias para poder responder a cada pregunta planteada.

El objetivo principal es ayudar a detectar las deficiencias y posibles mejoras de seguridad en la red, y a la vez, concienciar sobre la necesidad y facilidad de adoptarlas.

Una vez completado el check list, y habiendo obtenido las recomendaciones por las deficiencias encontradas, estos resultados se pueden exportar a un fichero de Excel que será almacenado en el dispositivo. De esta forma, el check list es manejable fuera de la aplicación e incluso del dispositivo.

- **Herramientas**

Se ofrecen una serie de herramientas útiles, bien para facilitar la respuesta de las preguntas del cuestionario, o para su uso de manera independiente.

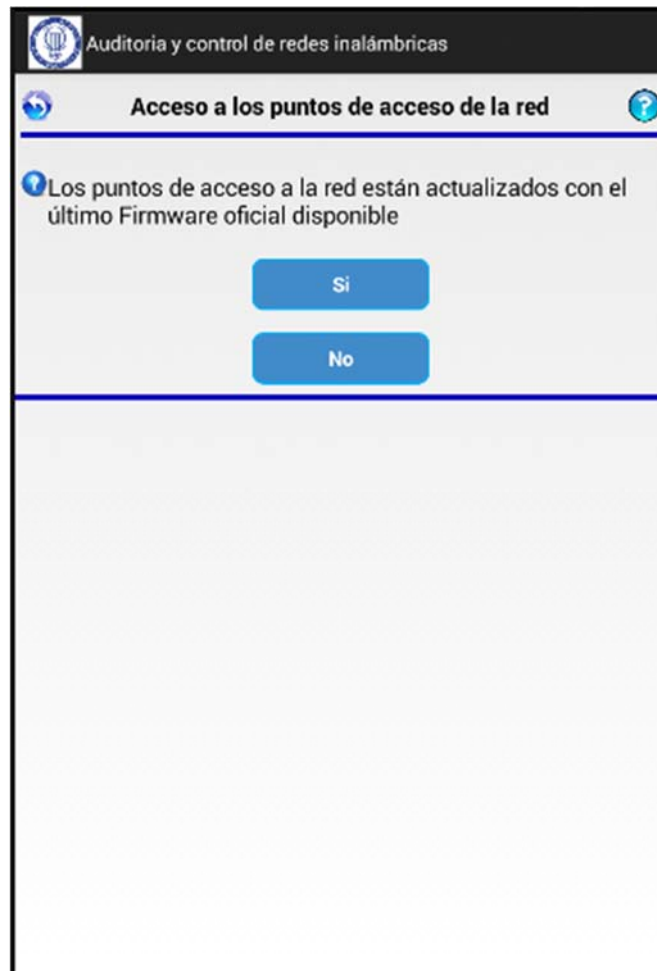
Las herramientas que se han implementado y están disponibles en esta versión son las que se listan a continuación, y se verán en detalle en los siguientes apartados.

- Wardriving
- Escaner
- Intensidad

9.2.3 Check list de seguridad inalámbrica

9.2.3.1 Nuevo check list

En cada pregunta se ofrece ayuda, y en caso de ser necesario, un acceso a las herramientas útiles para poder responder a la misma.



El prototipo muestra una interfaz de usuario para una pregunta de seguridad. En la parte superior, hay una barra de título con el logo de la Universidad Carlos III de Madrid y el texto "Auditoría y control de redes inalámbricas". Debajo de esto, hay una barra de sub-título con el texto "Acceso a los puntos de acceso de la red" y un icono de ayuda (punto de interrogación). La pregunta principal es "Los puntos de acceso a la red están actualizados con el último Firmware oficial disponible". Debajo de la pregunta, hay dos botones de respuesta: "Si" y "No".

Figura 41. Prototipo Preguntas

9.2.3.2 Listado de sesiones check list

Se muestra un listado con las sesiones de check list realizadas.

Cada sesión está identificada por su nombre y se indica su fecha de inicio y fin.

Además muestra un icono indicando el estado de la sesión:



Incompleta



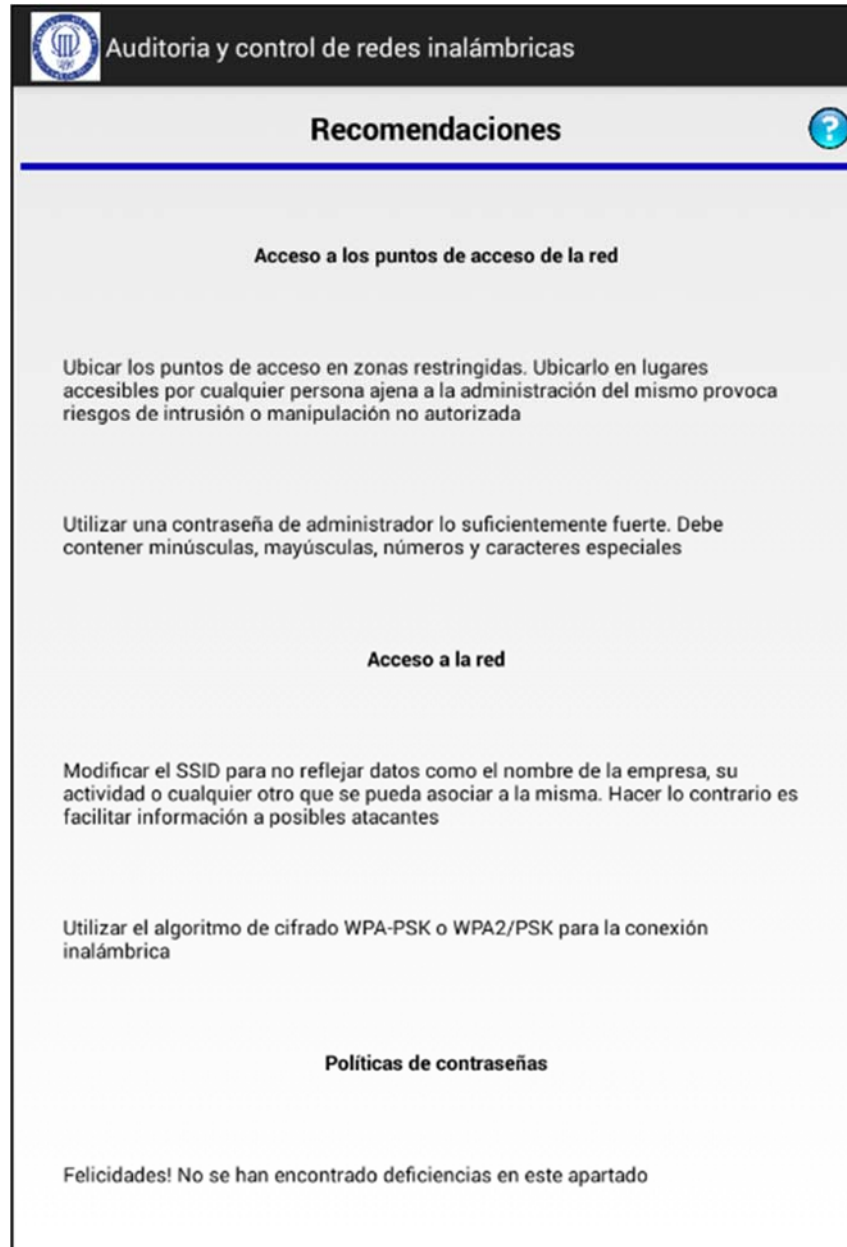
Finalizada

Sobre estas sesiones se pueden realizar una serie de operaciones:

- **Ver resultado:** Se muestra el resultado final con sus recomendaciones. Solo está disponible si la sesión ha sido finalizada.
- **Continuar:** Continúa con una sesión incompleta.
- **Editar nombre:** Edita el nombre de la sesión.
- **Eliminar sesión:** Borra la sesión de la base de datos.

9.2.3.3 Resultado del check list

Como resultado final se ofrece un informe con una serie de recomendaciones y puntos a mejorar en base a las respuestas del cuestionario.



El prototipo de pantalla muestra un informe de recomendaciones. En la parte superior, hay un encabezado con el logo de la Universidad Carlos III de Madrid y el título 'Auditoría y control de redes inalámbricas'. Debajo de esto, el título principal de la sección es 'Recomendaciones', acompañado de un icono de ayuda (un círculo azul con una interrogante). El contenido se organiza en secciones con títulos en negrita:

- Acceso a los puntos de acceso de la red**

Ubicar los puntos de acceso en zonas restringidas. Ubicarlo en lugares accesibles por cualquier persona ajena a la administración del mismo provoca riesgos de intrusión o manipulación no autorizada

Utilizar una contraseña de administrador lo suficientemente fuerte. Debe contener minúsculas, mayúsculas, números y caracteres especiales
- Acceso a la red**

Modificar el SSID para no reflejar datos como el nombre de la empresa, su actividad o cualquier otro que se pueda asociar a la misma. Hacer lo contrario es facilitar información a posibles atacantes

Utilizar el algoritmo de cifrado WPA-PSK o WPA2/PSK para la conexión inalámbrica
- Políticas de contraseñas**

Al final de la lista, se muestra un mensaje de felicitación: 'Felicidades! No se han encontrado deficiencias en este apartado'.

Figura 42. Prototipo Recomendaciones

A continuación se detalla cada pregunta (P) con su respectiva recomendación (R) en caso de que se detecte una deficiencia en la misma.

Acceso a los puntos de acceso de la red	
P	Los puntos de acceso a la red están actualizados con el último Firmware oficial disponible
R	Comprobar en la web del fabricante del hardware si existen actualizaciones del Firmware
P	Los puntos de acceso a la red están situados en zonas restringidas, siendo tan sólo accesibles por personal autorizado
R	Ubicar los puntos de acceso en zonas restringidas. Ubicarlo en lugares accesibles por cualquier persona ajena a la administración del mismo provoca riesgos de intrusión o manipulación no autorizada
P	El acceso remoto a la administración de los puntos de acceso a la red está restringido (solo desde LAN)
R	Restringir el acceso a la administración de los puntos de acceso a la red local. Tener abierta la administración a IPs externas o desde la WIFI provoca riesgos de intrusión o manipulación no autorizada
P	La contraseña de administrador de los puntos de acceso es modificada al menos cada 6 meses
R	Modificar la contraseña de administrador con frecuencia. Se evita que si un atacante ha conseguido obtenerla pueda utilizarla indefinidamente
P	La contraseña de administrador es segura. Contiene minúsculas, mayúsculas, números y caracteres especiales
R	Utilizar una contraseña de administrador lo suficientemente fuerte. Debe contener minúsculas, mayúsculas, números y caracteres especiales
P	La dirección IP de red local de los puntos de acceso ha sido modificada (no es la de por defecto)
R	Modificar la dirección IP de red local de los puntos de acceso para evitar que los atacantes conozcan de antemano direcciones IP
P	Los servicios, interfaces y protocolos sin uso o que no son estrictamente necesarios están deshabilitados

R	Deshabilitar los servicios, interfaces y protocolos sin uso o que no son estrictamente necesarios
P	Se apagan los puntos de acceso a la red si no se va a ser utilizados en periodos de tiempo prolongados
R	Apagar los puntos de acceso si no se va a usar en periodos de tiempo prolongados, como por ejemplo en periodos vacacionales o fines de semana

Acceso a la red	
P	El SSID refleja datos identificativos de la empresa o su actividad
R	Modificar el SSID para no reflejar datos como el nombre de la empresa, su actividad o cualquier otro que se pueda asociar a la misma. Hacer lo contrario es facilitar información a posibles atacantes
P	Se propaga el SSID o nombre de la red
R	Deshabilitar la propagación del SSID. Al propagarlo permite conocer la existencia de la red y sus características a cualquier posible intruso
P	La intensidad de la señal se ajusta a los límites físicos de la organización
R	Reubicar los puntos de acceso con el fin de que la señal exceda lo menos posible los límites físicos externos de la organización
P	La red tiene en todo momento habilitado un algoritmo de cifrado
R	Utilizar un algoritmo de cifrado para impedir el acceso a la red
P	Se utiliza el algoritmo de cifrado WPA-PSK o WPA2/PSK
R	Utilizar el algoritmo de cifrado WPA-PSK o WPA2/PSK para la conexión inalámbrica
P	Los puntos de acceso tienen la opción de filtrado por MAC habilitada
R	Activar la opción de filtrado por MAC en los puntos de acceso a la red
P	Los administradores de red mantienen un listado con la MAC de todos los equipos cliente de la red
R	Mantener un listado actualizado con todos los equipos que se pueden conectar a la red

P	Se define en los puntos de acceso a la red un número máximo de dispositivos que pueden conectar a ellos
R	Establecer un máximo de dispositivos que se pueden conectar a la red acorde a la realidad de la empresa
P	Los puntos de acceso a la red tienen el servicio WPS deshabilitado
R	Deshabilitar el servicio WPS, si está activado puede ser utilizado para conectar a la red sin necesidad de conocer la contraseña
P	Los puntos de acceso a la red tienen el servicio DHCP deshabilitado
R	Deshabilitar la opción DHCP. En la medida de lo posible, es recomendable tener IPs fijas asignadas a cada cliente de la red

Políticas de contraseñas	
P	La contraseña de acceso a la red es segura. Contiene minúsculas, mayúsculas, números y caracteres especiales
R	Modificar la contraseña de acceso a la red. Debe contener minúsculas, mayúsculas, números y caracteres especiales
P	Las contraseñas son modificadas al menos cada 6 meses
R	Modificar la contraseña de acceso a la red con frecuencia. Se evita que si un atacante ha conseguido obtenerla, no pueda utilizarla indefinidamente. Además dificulta la captura de gran cantidad de tráfico cifrado con la misma contraseña
P	Existen políticas de comunicación de contraseña adecuadas
R	Establecer mecanismos y políticas de comunicación de contraseña para los empleado

Usuarios y equipos cliente de la red	
P	Los usuarios de la red tienen apuntadas las contraseñas en lugares visibles o en ficheros en claro almacenados en el ordenador

R	Controlar que hay contraseñas anotadas en lugares visibles al alcance de cualquier persona no autorizada
P	Los equipos cliente de la red se actualizan con los parches de seguridad recomendados
R	Revisar periódicamente por parte de los administradores de sistemas que los parches de seguridad recomendados están instalados
P	Los equipos cliente de la red tienen antivirus instalados y son actualizados periódicamente
R	Revisar periódicamente por parte de los administradores de sistemas que los antivirus están al día
P	Los equipos cliente de la red tienen los firewall personales habilitados
R	Habilitar los firewall en los equipos cliente de la red
P	Los equipos cliente de la red tienen contraseña para el inicio de sesión
R	Establecer contraseñas de inicio de sesión en los equipos cliente
P	Modo ad-hoc está deshabilitado en todos los equipos
R	Deshabilitar el modo ad-hoc en todos los equipos

Políticas de revisión de logs	
P	Existe política de revisión de logs de acceso en los puntos de acceso a la red
R	Revisar periódicamente los logs en los elementos de acceso a la red para detectar intentos de intrusión y prevenir futuros ataques

Este resultado se puede exportar a un fichero de Excel que será almacenado en el dispositivo. De esta forma, el check list es manejable fuera de la aplicación e incluso del dispositivo.

El excel resultante es como se muestra a continuación:

Pregunta	Respuesta	Recomendación
1. Los puntos de acceso a la red están actualizados con el último Firmware oficial disponible	No	Comprobar en la web del fabricante del hardware si existen actualizaciones del Firmware
2. Los puntos de acceso a la red están situados en zonas restringidas, siendo tan sólo accesibles por personal autorizado	No	Revisar los puntos de acceso en zonas restringidas. Ubicarlos en lugares accesibles por cualquier persona ajena a la administración del mismo, prevea riesgos de intrusión o manipulación
3. Los puntos de acceso a la red tienen un nivel de seguridad mínimo de 128 bits (WPA2 o WPA3)	No	Revisar los puntos de acceso en zonas restringidas. Ubicarlos en lugares accesibles por cualquier persona ajena a la administración del mismo, prevea riesgos de intrusión o manipulación
4. La contraseña de administrador de los puntos de acceso es modificada al menos cada 6 meses	No	Modificar la contraseña de administrador con frecuencia. Se evita que si un atacante ha conseguido obtenerla pueda utilizarla indefinidamente
5. La contraseña de administrador es segura. Contiene minúsculas, mayúsculas, números y caracteres especiales	No	Utilizar una contraseña de administrador lo suficientemente fuerte. Deba contener minúsculas, mayúsculas, números y caracteres especiales
6. La dirección IP de red local de los puntos de acceso ha sido modificada (no es la de por defecto)	No	Modificar la dirección IP de red local de los puntos de acceso para evitar que los atacantes conozcan de antemano direcciones IP
7. Los servicios, interfaces y protocolos sin uso o que no son estrictamente necesarios están deshabilitados	No	Deshabilitar los servicios, interfaces y protocolos sin uso o que no son estrictamente necesarios
8. Se apagan los puntos de acceso a la red si no se va a ser utilizados en periodos de tiempo prolongados	No	Apagar los puntos de acceso si no se va a usar en periodos de tiempo prolongados, como por ejemplo en periodos vacacionales o fines de semana
9. El SSID refleja datos identificativos de la empresa o su actividad	Si	Modificar el SSID para no reflejar datos como el nombre de la empresa, su actividad o cualquier otro que se pueda asociar a la misma. Hacer lo contrario es facilitar información a posibles atacantes
10. La intensidad de la señal se ajusta a los límites físicos de la organización	No	Deshabilitar la propagación del SSID. Al propagarlo permite conocer la existencia de la red y sus características a cualquier posible intruso
11. Se propaga el SSID o nombre de la red	Si	Reubicar los puntos de acceso con el fin de que la señal exceda lo menos posible los límites físicos externos de la organización
12. La red tiene en todo momento habilitado un algoritmo de cifrado	No	Utilizar un algoritmo de cifrado para impedir el acceso a la red
13. Se utiliza el algoritmo de cifrado WPA-PSK o WPA2-PSK	Si	Activar la opción de filtrado por MAC en los puntos de acceso a la red
14. Los puntos de acceso tienen la opción de filtrado por MAC habilitada	No	Mantener un listado actualizado con todos los equipos que se pueden conectar a la red
15. Se define en los puntos de acceso a la red un número máximo de dispositivos que pueden conectar a ellos	No	Deshabilitar el servicio WPS, si está activado puede ser utilizado para conectar a la red sin necesidad de conocer la contraseña
16. Los puntos de acceso a la red tienen el servicio DHCP deshabilitado	Si	
17. La contraseña de acceso a la red tiene el servicio DHCP deshabilitado	No	
18. Los puntos de acceso a la red tienen el servicio DHCP deshabilitado	Si	
19. Los puntos de acceso a la red tienen el servicio DHCP deshabilitado	No	
20. La contraseña de acceso a la red es segura. Contiene minúsculas, mayúsculas, números y caracteres especiales	Si	
21. Las contraseñas son modificadas al menos cada 6 meses	No	Establecer mecanismos y políticas de comunicación de contraseña para los empleados
22. Existen políticas de comunicación de contraseñas adecuadas	No	Controlar que hay contraseñas anotadas en lugares visibles al alcance de cualquier persona no autorizada
23. Los usuarios de la red tienen apuntadas las contraseñas en lugares visibles o en ficheros en claro almacenados en el ordenador	Si	Revisar periódicamente por parte de los administradores de sistemas que los parches de seguridad recomendados están instalados
24. Los usuarios de la red se actualizan con los parches de seguridad recomendados	No	Revisar periódicamente por parte de los administradores de sistemas que los parches de seguridad recomendados están instalados
25. Los equipos cliente de la red tienen antivirus instalados y son actualizados periódicamente	No	Habilitar los firewall en los equipos cliente de la red
26. Los equipos cliente de la red tienen los firewall personales habilitados	No	Establecer contraseñas de inicio de sesión en los equipos cliente
27. Los equipos cliente de la red tienen todos los servicios de red deshabilitados	No	Revisar periódicamente los logs en los elementos de acceso a la red para detectar intentos de intrusión y prevenir futuros ataques
28. Los equipos cliente de la red tienen todos los servicios de red deshabilitados	No	
29. Existe política de revisión de logs de acceso en los puntos de acceso a la red	No	

9.2.4 Herramientas

La aplicación dispone de una serie de herramientas orientadas al análisis de redes.

9.2.4.1 WarDriving

Permite realizar wardriving. Es decir, escanear las redes disponibles con la frecuencia de tiempo configurada mientras nos desplazamos físicamente.

Las redes detectadas pueden ser almacenadas para su consulta posterior, y ubicadas en el mapa.



Figura 43. Prototipo WarDriving

Si se selecciona la opción “Ver sesiones”, aparece una lista de todas las sesiones de wardriving realizadas, ordenadas por fecha.

Sobre cada una de ellas se permite una serie de acciones:

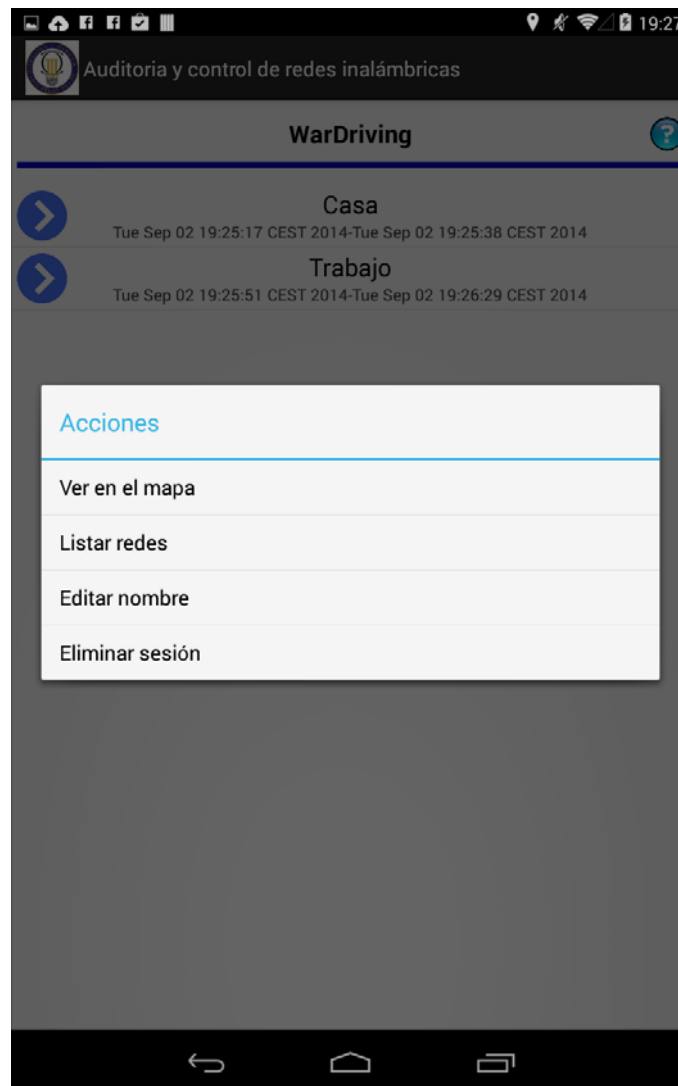


Figura 44. Prototipo WarDriving opciones

- **Ver en el mapa:** Sitúa las redes detectadas sobre el mapa. Las redes se agrupan por colores según el protocolo de cifrado utilizado. Siendo:



Abierta



WEP



WPA



WPA2

- **Listas redes:** Lista las redes detectadas en la sesión. En el listado de redes se ofrece la posibilidad de ubicar una red concreta sobre el mapa.
- **Editar nombre:** Edita el nombre de la sesión.
- **Eliminar sesión:** Elimina la sesión de la base de datos.

A continuación se muestra un ejemplo de ubicación sobre el mapa:



Figura 45. Prototipo WarDriving Mapa

9.2.4.2 Escaner wifi

Realiza un escaneo de las redes disponibles obteniendo para cada una de ellas la siguiente información:

- **Intensidad de la señal:** Varía entre seis niveles:



- **SSID y BSSID**
- **Tipo de cifrado:**



A continuación se muestra un ejemplo de un listado de redes wifi detectadas en el escaner:



Figura 46. Prototipo Escáner

9.2.4.3 Medidor intensidad de señal

Introducido el nombre de la red a medir, realiza un escaneo de la intensidad de la señal de dicha red, actualizándose con la frecuencia de tiempo configurada.

Los niveles de intensidad se corresponden a los ya mencionados anteriormente.

A continuación se muestra un ejemplo del medidor de intensidad:

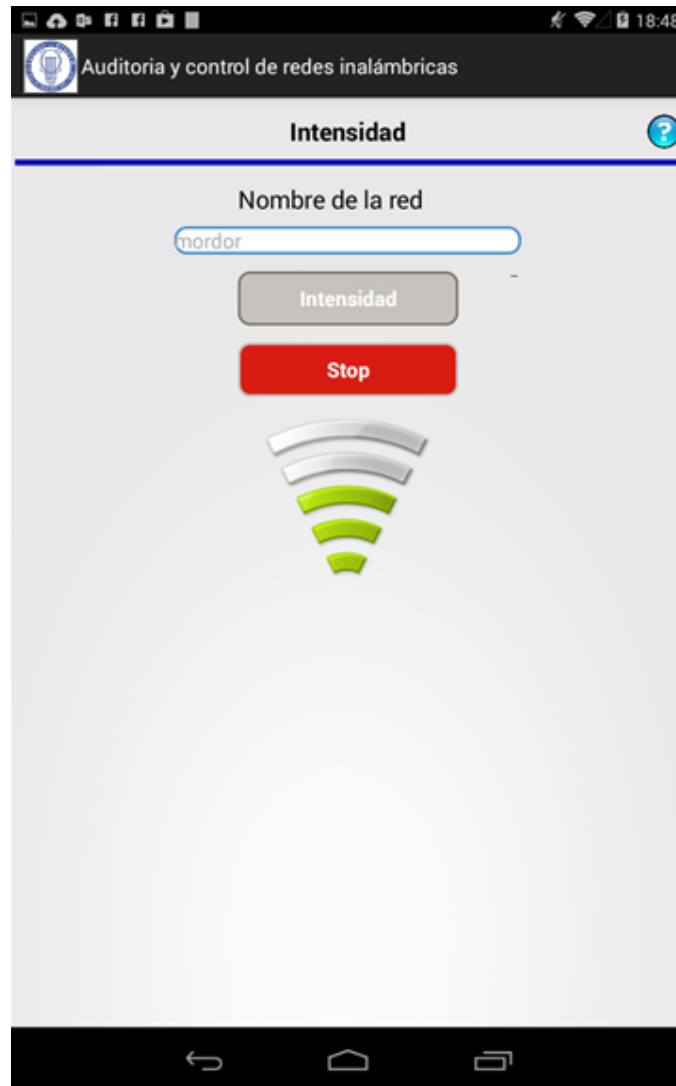


Figura 47. Prototipo Intensidad de señal

9.3 Detalles de implementación

La aplicación ha sido implementada teniendo en cuenta la metodología de diseño MVC (Modelo-Vista-Controlador) que consiste en separar de una manera clara los datos de la aplicación, la interfaz de usuario y la lógica de negocio.

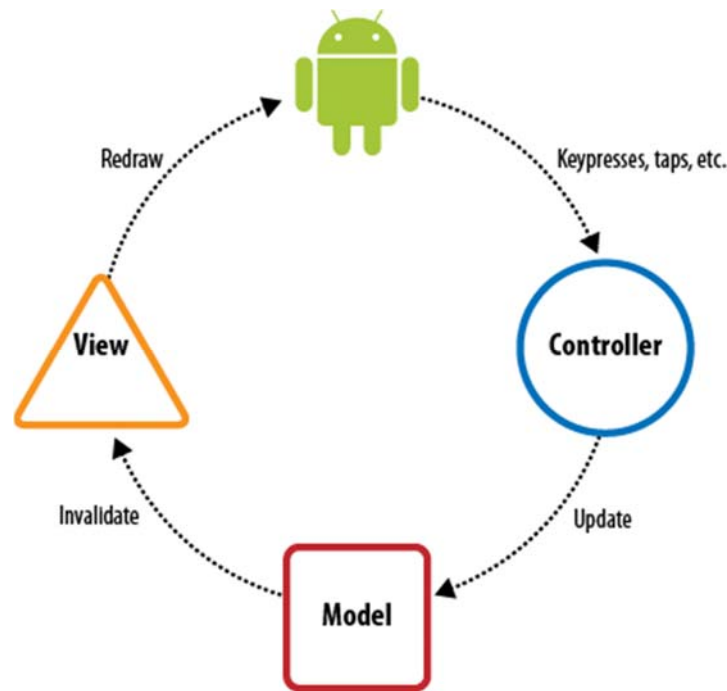


Figura 48. Modelo Vista Controlador en Android

De esta forma es más sencillo separar las tareas de desarrollo para la realización de componentes específicos que pueden ser reutilizables desde diferentes puntos o incluso en futuros proyectos.

- **Modelo:** Representación de la información que se maneja en la aplicación.
- **Vista:** Esqueleto visual que se presentará al usuario para su interacción.
- **Controlador:** Clases o manejadores que permiten completar la interfaz gráfica, y consumir la información proporcionada por el usuario.

9.3.1 Modelo

Como hemos comentado anteriormente, el modelo es la representación de la información que utiliza la aplicación, o en otras palabras, los objetos físicos o lógicos que utilizará.

Para almacenar la información del modelo se utiliza una base de datos relacional, que se detalla a continuación.

9.3.1.1 Base de datos

Se ha utilizado la base de datos SQLite que trae embedida Android.

Se requiere el uso de una base de datos para almacenar la información de dos de las funcionalidades de la aplicación:

- **Sesiones Check List:** Las sesiones del cuestionario o check list son almacenadas en la base de datos para poder:
 - Continuar el cuestionario en otro momento, no siendo necesario realizarlo completo de una sola vez.
 - Recuperación ante posibles errores, de forma que se guarda automáticamente el progreso del check list.
 - Una vez respondidas todas las preguntas del check list, poder recuperar el resultado de la auditoría y exportarla a Excel.

El modelo necesario se detalla en el siguiente diagrama de Entidad-Relación:

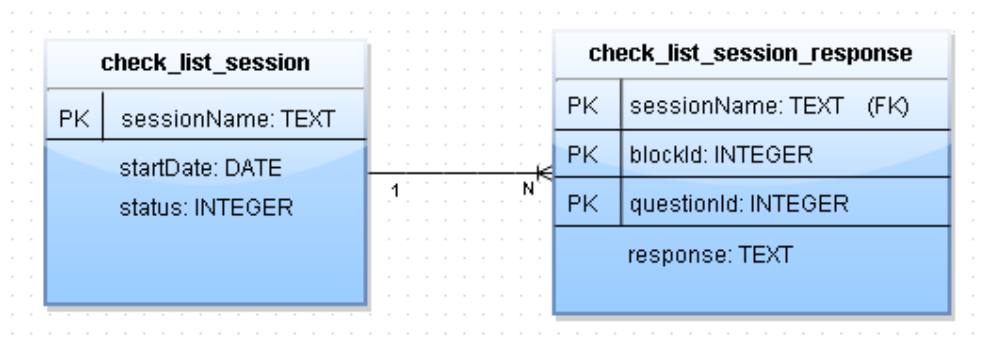


Figura 49. Modelo E-R. Sesiones Check List

- **Sesiones wardriving:** Se almacenan las sesiones de la herramienta de wardriving, así como las redes inalámbricas que va encontrando.

El modelo necesario se detalla en el siguiente diagrama de Entidad-Relación:

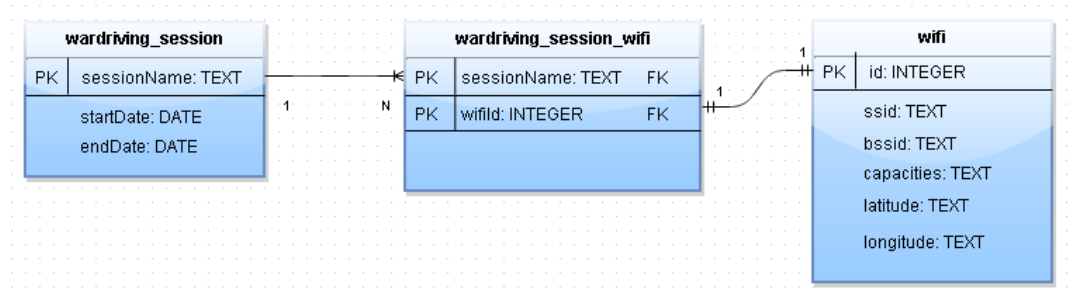


Figura 50. Modelo E-R. Sesiones wardriving

9.3.2 Vista

Es la interfaz con la que va a interactuar el usuario. En esta parte se utiliza lenguaje XML.

9.3.2.1 Layout

El interfaz visual de la aplicación se basa en ficheros plantilla XML conocidos como ficheros de Layout.

Para entendernos, un Layout es la ventana que el usuario ve en la pantalla de su dispositivo, en la que se definen elementos como pueden ser los botones, iconos, textos entre otros.

Estas plantillas serán utilizadas, dándoles forma y vida por lo que se denomina Activities que serán explicadas en el apartado Controlador.

Con el fin de optimizar los cambios y evitar repetir código se ha separado lo máximo posible cada elemento visual de cada pantalla, de tal forma que se ha generado una plantilla para cada una de las partes. De esta forma se puede utilizar la misma plantilla sin necesidad de repetir código, personalizando textos, desde diferentes pantallas de la aplicación.

A continuación se detallan las diferentes pantallas o layouts generadas para la aplicación:

- **Pantalla principal**

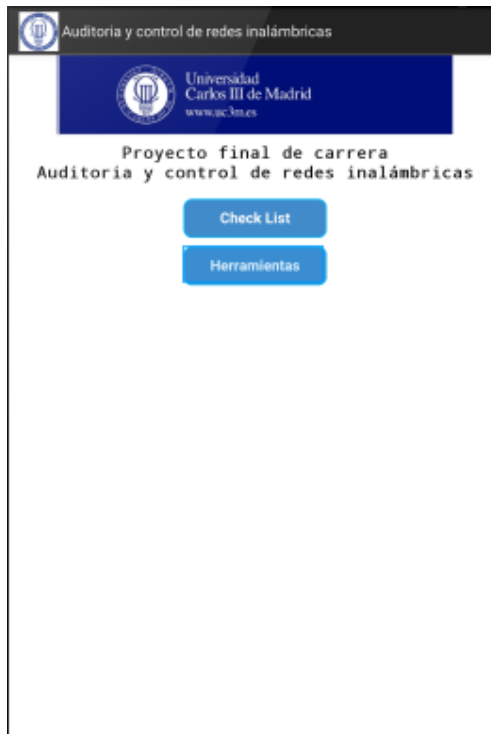


Figura 51. activity_main.xml

- **Cuestionario**

Plantilla que se utiliza en cada una de las pantallas del cuestionario.

Se compone de las plantillas common_cabecera.xml, checklist_pregunta.xml, checklist_respuesta.xml y checklist_cuestionario_ayuda_adicional.xml

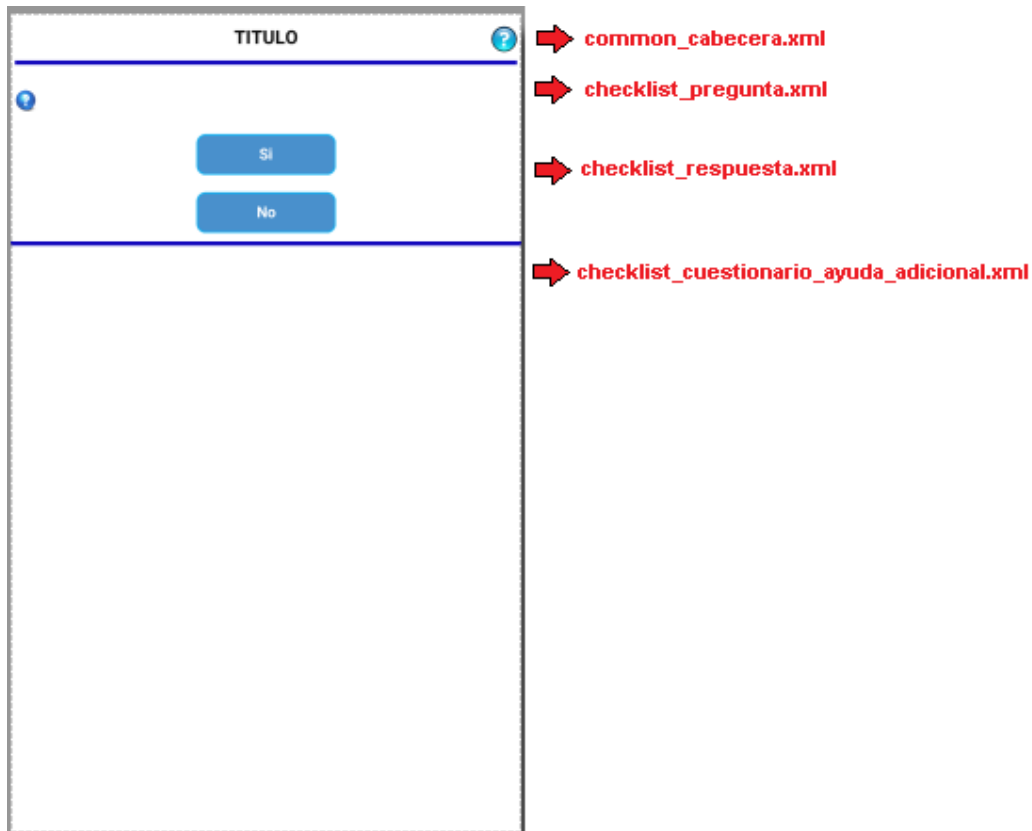


Figura 52. checklist_cuestionario.xml

Aspecto una vez rellenada dinámicamente:

The screenshot shows a mobile application interface titled 'Auditoría y control de redes inalámbricas'. The main section is 'Acceso a la red'. It contains a question: 'El SSID refleja datos identificativos de la empresa o su actividad'. Below the question are two buttons: 'Si' and 'No'. Below these buttons is a section titled 'Comprobar las características con la red con la herramienta de escaner' with a button labeled 'Escanear'. To the right of the interface, red arrows point to specific XML files: 'common_cabecera.xml' points to the top bar, 'checklist_pregunta.xml' points to the question text, 'checklist_respuesta.xml' points to the 'Si' and 'No' buttons, and 'checklist_cuestionario_ayuda_adicional.xml' points to the 'Escanear' button.

Figura 53. checklist_cuestionario.xml

- **Resultado**

La plantilla de resultado es muy básica, ya que se rellena prácticamente en su totalidad de forma dinámica en función de las respuestas del cuestionario.

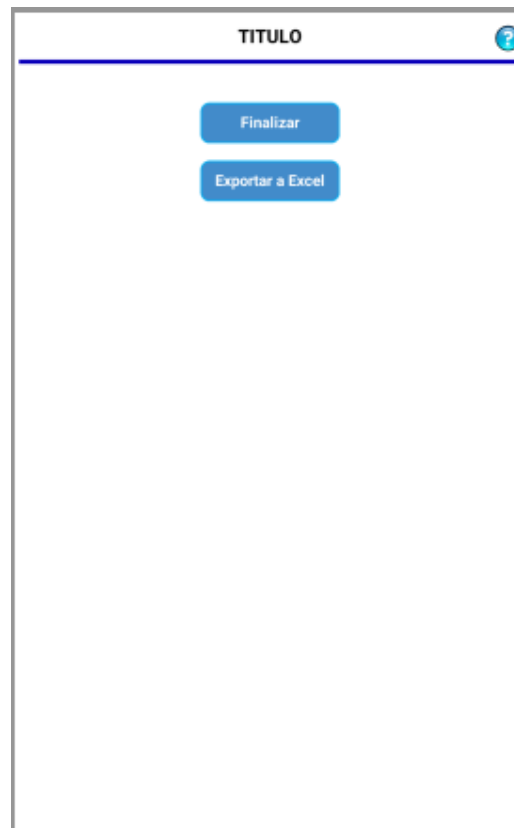


Figura 54. checklist_resultado.xml

9.3.2.2 Recursos

En la programación para Android, es muy importante el concepto de recurso. Independientemente del tipo que sea (texto, imagen, color, etc) a cada recurso previamente definido, se le asigna un identificador único, por el que será referenciado cuando se utilice.

La forma de utilizar un recurso es diferente según se utilice desde la plantilla XML o desde el código Java que la recubre y completa.

Desde la plantilla XML se utiliza un tag dependiendo del tipo de recurso, de la siguiente forma: @tipo/nombre. A continuación se detalla un ejemplo:

```
<ImageView
    android:background="@drawable/asteroide"
    android:text="@string/texto"
    android:text_color="@color/verde"/>
```

Desde clases Java se utiliza el método getResources para obtener los recursos de la aplicación y sobre ellos se obtiene el tipo deseado como se ve en el siguiente ejemplo:

```
Resources res = getResources();
Drawable drawable = res.getDrawable(R.drawable.asteroide);
String saludo = res.getString(R.string.texto);
```

Tabla de uso de recurso según el tipo:

Tipo	XML	JAVA
Imagen	@drawable/<recurso>	getDrawable(R.drawable.<recurso>);
Texto	@string/<recurso>	getString(R.string.<recurso>);
Color	@color/<recurso>	getColor (R.color.<recurso>);
Estilo	@style/<recurso>	getStyle (R.style.<recurso>);

9.3.2.3 Imágenes

Comprende todos los iconos, logos y otras imágenes que muestra la aplicación.

9.3.2.4 Textos, estilos, colores y valores

Todos los textos, estilos, colores y valores que se utilizan en la aplicación están contenidos en los ficheros de recursos XML que se listan a continuación:

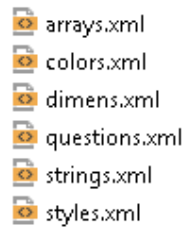


Figura 55. Recursos. Textos, estilos y valores

De esta forma si se quiere modificar el texto de una pregunta del check list sería tan sencillo como editar el recurso questions.xml, si se desea modificar un texto propio de la aplicación el recurso strings.xml, y así sucesivamente.

Los XML son estándar y tienen la siguiente forma:

```
<string name="ok">OK</string>
```

9.3.3 Controlador

El controlador es la parte que da vida a la aplicación.

Entre otras cosas, complementa la parte visual, consume las acciones o la información proporcionada por el usuario y define qué hacer con ello.

El módulo de controlador se compone de lo que se denominan actividades o Activities y son desarrollarlos en lenguaje Java.

9.3.3.1 Activity

De una manera muy genérica se puede decir que cada pantalla de la aplicación se corresponde a lo que se denomina como un Activity.

Una Activity tiene una parte lógica (clase java) y una parte gráfica asociada a un layout (xml). La asociación se hace en el elemento onCreate con la función “setContentView”, de la siguiente forma:

```
@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.checklist_main);
}
```

El funcionamiento interno de una actividad o Activity, se detalla en el siguiente flujograma:



Figura 56. Flujograma de un Activity

9.3.3.2 GPSTracker

Para determinar la ubicación de la red inalámbrica detectada se ha implementado una clase GPSTracker que actualiza la ubicación del dispositivo cada 10 segundos o cuando ocurre un cambio de 10 metros de distancia.

Así, en una sesión de wardriving, se conoce la ubicación del dispositivo en todo momento, y de tal manera se asocia esa ubicación a la red inalámbrica detectada.

Para determinar la ubicación se utiliza localización por red y por GPS, priorizando la determinada por GPS en caso de estar la opción activada en el dispositivo.

9.3.3.3 Google Maps

Para mostrar la ubicación de las redes en la herramienta wardriving se ha utilizado el API de Google Maps.

9.4 Pruebas del prototipo

Se han realizado diferentes fases pruebas tanto durante el ciclo de vida del desarrollo (pruebas unitarias), como sobre la versión final del software (pruebas end-to-end).

Dichas pruebas abarcan toda la funcionalidad con el fin de validar el comportamiento global de la aplicación, así como que cumple con todos los requisitos definidos durante la fase de análisis.

9.5 Futuras mejoras del prototipo

- Personalización del check list a partir de un fichero de entrada

La aplicación dará la opción de basar su check list en función de un Excel de entrada con un formato específico (similar al de salida).

De esta manera se tendrá disponible el check list programado por defecto, y los diferentes check list personalizados.

- Nuevas herramientas
 - Ataque por diccionario o fuerza bruta

Realizará intentos de conexión bien por diccionario o fuerza bruta a una red inalámbrica.

- Descubrir equipos en la misma red

Sondeará las IPs de la red local en busca de otros equipos conectados.

Capítulo 10

Planificación y Presupuesto

Este capítulo detalla la planificación del proyecto mediante un diagrama de Gantt, así como la realización de un presupuesto de estimación de costes.

10.1 Planificación

Para realizar la planificación del proyecto se ha utilizado un diagrama Gantt realizado con la herramienta de gestión de proyectos ProjectLibre.

La planificación se ha ido ajustando a lo largo del desarrollo del proyecto ajustándose a las desviaciones de tiempo respecto a la planificación inicial.

El motivo de dichas desviaciones de tiempo viene asociado a la necesidad de compaginar la realización del proyecto con la actividad laboral, que en determinados momentos, por carga de trabajo y/o por viajes laborales ha impactado de manera significativa en las estimaciones iniciales.

En la siguiente figura que contiene la planificación del proyecto completo. Teniendo en cuenta que cada día de trabajo corresponden a dos horas de dedicación.

	Nombre	Duracion	Inicio	Terminado	Predecesores
1	Inicio del proyecto	0 days	1/10/14 8:00	1/10/14 8:00	
2	Fase de documentación teórica	210 days	2/10/14 8:00	22/07/15 17:00	
3	Prototipo	188 days	3/11/14 8:00	22/07/15 17:00	
4	Fase de análisis	5 days	3/11/14 8:00	7/11/14 17:00	
5	Análisis de requisitos	5 days	3/11/14 8:00	7/11/14 17:00	
6	Fase de diseño	20 days	10/11/14 8:00	5/12/14 17:00	4
7	Diseño interfaz gráfico	20 days	10/11/14 8:00	5/12/14 17:00	
8	Diseño BD	5 days	10/11/14 8:00	14/11/14 17:00	
9	Fase de implementación	45 days	8/12/14 8:00	6/02/15 17:00	6
10	Implementación de la aplicación	45 days	8/12/14 8:00	6/02/15 17:00	
11	Fase de documentación del prototipo	20 days	9/02/15 8:00	6/03/15 17:00	9
12	Documentación del prototipo	20 days	9/02/15 8:00	6/03/15 17:00	9
13	Fin del proyecto	0 days	22/07/15 17:00	22/07/15 17:00	2

Figura 57. Planificación

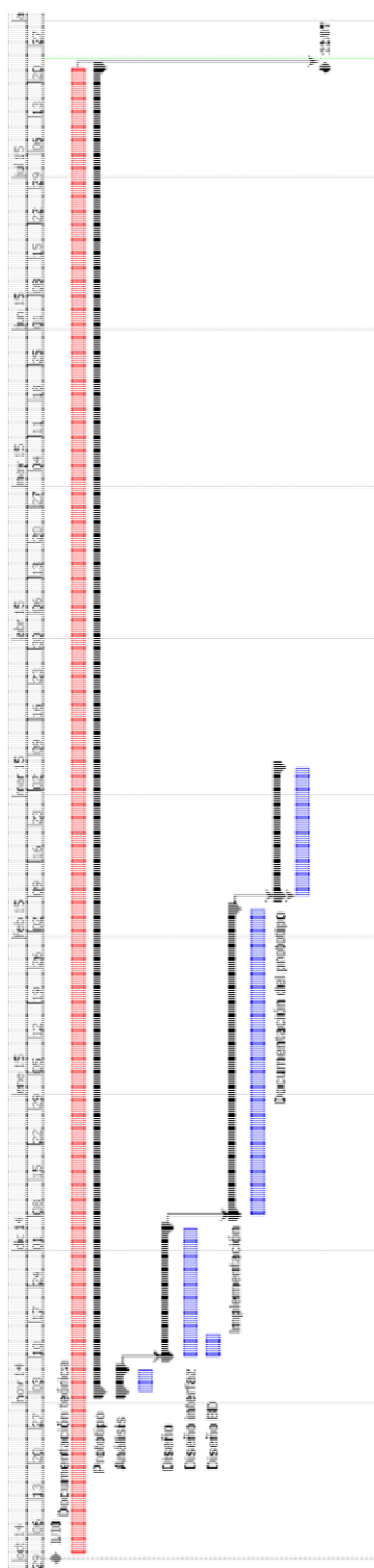


Figura 58. Diagrama Gantt

10.2 Presupuesto

En este apartado se detalla el presupuesto del proyecto, especificando el gasto de personal, de software y de hardware.

Para su realización se han utilizado las plantillas proporcionadas por la UC3M.

10.2.1 Horas dedicadas

A partir de la planificación expuesta en el apartado anterior, es posible calcular el número de horas totales dedicadas a la realización del proyecto

- Documentación: $210 \text{ días} * 2 \text{ hora/día} = 420 \text{ horas}$
- Fase de análisis: $5 \text{ días} * 2 \text{ horas/día} = 10 \text{ horas}$
- Fase de diseño: $25 \text{ días} * 2 \text{ horas/día} = 50 \text{ horas}$
- Fase de implementación: $45 \text{ días} * 2 \text{ horas/día} = 90 \text{ horas}$
- Documentación del prototipo: $20 \text{ días} * 2 \text{ hora/día} = 40 \text{ horas}$

Por tanto el número de horas totales dedicadas al proyecto es la suma de las horas dedicadas a cada una de las fases.

Siendo el coste total en horas de 610 horas.

10.2.2 Coste de personal

En la siguiente tabla se muestran los costes correspondientes al personal necesario para realizar las distintas tareas del proyecto.

El coste por hora es acorde a los salarios de empleados con los mismos perfiles en empresas del sector. Todos los costes son calculados sin I.V.A.

Puesto	Nº de horas	Coste / hora	Dedicación en meses*	Total (€)
Analista	10	30 €	0,25	300
Diseñador	50	30 €	1,25	1500
Programador	90	20 €	2,5	1800
Responsable de documentación	460	15 €	11,5	6900
Total	610			10500

Tabla 3. Coste de personal

*Utilizando 1 Hombre/ mes = 40 horas según la planificación realizada

10.2.3 Coste de software

En la siguiente tabla se muestran las herramientas software utilizadas para la realización del proyecto.

Todos los costes son calculados sin I.V.A

Descripción	Coste imputable (€)
Microsoft Office 2013 Professional	250
ProjectLibre	0
Microsoft Office Visio 2013	100
Android Studio	0
Total	350

Tabla 4. Coste de software

10.2.4 Coste de hardware

En la siguiente tabla se muestran los equipos informáticos y hardware utilizados con su coste de amortización durante el periodo que dura el proyecto.

Todos los costes son calculados sin I.V.A.

Descripción	Coste (€)	% uso dedicado	Dedicación en meses	Periodo de depreciación	Coste / Mes	Coste imputable (€)
Portatil HP ProBook 6460b	399	100	12	60	6,65	79,80
Impresora HP Deskjet 2540	50	100	12	60	0,83	10
Pendrive 32 Gb	15	100	12	60	0,25	3
Teclado y ratón	25	100	12	36	0,69	8,33
Teléfono Samsung S3 Mini	200	100	12	36	5,55	66,66
Total						167,80

Tabla 5. Coste de hardware

10.2.5 Coste de material fungible

En la siguiente tabla se muestra el coste del material fungible que se estima necesario para la realización del proyecto.

Todos los costes son calculados sin I.V.A.

Descripción	Coste imputable (€)
Material de oficina	50
Recambios de impresora	30
Total	80

Tabla 6. Coste de material fungible

10.2.6 Resumen de costes

Por último, en la siguiente tabla, se muestra un resumen y el sumatorio de los totales anteriormente detallados. A lo cual se le incluye una tasa del 20 % en concepto de costes indirectos, equilibrando así los riesgos del proyecto y aquellos conceptos que no se hayan tenido en cuenta en la realización de este presupuesto.

Descripción	Costes totales (€)
Personal	10500
Costes de software	350
Amortización de hardware	167,79
Costes de material fungible	80
Costes indirectos (20%)	2219,558
Total	13317,348


Tabla 7. Resumen de costes

Finalmente se detalla el coste total del presupuesto aplicando el IVA actual del 21%.

Descripción	Costes totales (€)
Total sin IVA	13317,35
IVA 21%	2796,64
Total con IVA	16113,99

Tabla 8. Resumen de costes con IVA

10.2.7 Plantilla de presupuesto

 UNIVERSIDAD CARLOS III DE MADRID Escuela Politécnica Superior							
PRESUPUESTO DE PROYECTO							
1.- Autor:		Daniel Arnaiz Rubio					
2.- Departamento:		Informática					
3.- Descripción del Proyecto:							
- Título		Auditoría y control de redes inalámbricas					
- Duración (meses)		12					
Tasa de costes Indirectos:		20%					
4.- Presupuesto total del Proyecto (valores en Euros):							
13.317,36 Euros							
5.- Desglose presupuestario (costes directos)							
PERSONAL							
Apellidos y nombre	N.I.F. (no rellenar - solo a título informativo)	Categoría	Dedicación (hombres mes) ^{a)}	Coste hombre mes	Coste (Euro)	Firma de conformidad	
Arnaiz Rubio, Daniel		Analista	0,25	1.200,00	300,00		
Arnaiz Rubio, Daniel		Diseñador	1,25	1.200,00	1.500,00		
Arnaiz Rubio, Daniel		Programador	2,25	800,00	1.800,00		
Arnaiz Rubio, Daniel		Documentación	11,5	600,00	6.900,00		
Hombres mes 15,25				Total	10.500,00		
^{a)} 1 Hombre mes = 40 horas según la planificación realizada de 2 horas diarias de Lunes a Viernes							
EQUIPOS							
Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable ^{d)}		
Portatil HP ProBook 6460b	399,00	100	12	60	79,80		
Impresora HP Deskjet 2540	50,00	100	12	60	10,00		
Pendrivel 32 Gb	15,00	100	12	60	3,00		
Teclado y ratón	25,00	100	12	36	8,33		
Teléfono Samsung S3 Mini	200,00	100	12	36	66,67		
Total					167,80		
^{d)} Fórmula de cálculo de la Amortización:							
A		A = nº de meses desde la fecha de facturación en que el equipo es utilizado					
B		B = periodo de depreciación (60 meses)					
C		C = coste del equipo (sin IVA)					
D		D = % del uso que se dedica al proyecto (habitualmente 100%)					
SUBCONTRATACIÓN DE TAREAS							
Descripción	Empresa	Coste imputable					
Total					0,00		
OTROS COSTES DIRECTOS DEL PROYECTO ^{e)}							
Descripción	Empresa	Costes imputable					
Software		350,00					
Fungible		80,00					
Total					430,00		
^{e)} Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas.							
6.- Resumen de costes							
Presupuesto Costes Totales	Presupuesto Costes Totales						
Personal	10.500						
Amortización	168						
Subcontratación de tareas	0						
Costes de funcionamiento	430						
Costes Indirectos	2.220						
Total	13.317						

Capítulo 11

Futuras líneas de investigación

Como hemos visto a lo largo de este trabajo, las redes inalámbricas están en un momento álgido, y por la buena acogida del público en general hace pensar que seguirán estándolo en un futuro próximo.

Esto propicia que tanto los gobiernos como las empresas pongan gran énfasis en mejorar este tipo de tecnología. Por lo que es de prever que en un corto periodo de tiempo surjan diferentes evoluciones y nuevas tecnologías en este campo.

Actualmente ya se habla de algunas novedades que podrán llegar pronto, como son:

- **Li-Fi (*Light Fidelity*):** Es el término usado para etiquetar a los sistemas de comunicaciones inalámbricas rápidos y de bajo costo, el equivalente óptico al Wi-Fi.

La tecnología también es conocida como Comunicaciones de Luz Visible (VLC) y se ha comprobado que es capaz de alcanzar una velocidad de transmisión de datos de 10 Gbps.

El sistema Li-Fi usa una luz normal acoplada a una conexión a Internet que permite enviar datos a un receptor instalado en una computadora, se prevé que pronto se conviertan en un serio competidor del Wi-Fi en el mundo del Internet inalámbrico.

Como punto negativo conocido de momento, es que tanto el dispositivo que emite como el que recibe, tienen que estar en la misma habitación para que sea capaz de detectar la transmisión de luz.

- **IEEE 802.22 (*Super Wi-Fi*):** A diferencia del Wi-Fi actual que utiliza frecuencias de GHz, este nuevo estándar baja la frecuencia hasta los MHz, o lo que es lo mismo, la misma banda de frecuencia que para la transmisión de señales de televisión. Ya que cuanto menor es la frecuencia menor es la atenuación de la señal y, por tanto, más inmune es a obstáculos y más amplio rango de cobertura (hasta 8 kilómetros).

- **UWB (*Ultra Wide Band*)**: Es una tecnología de radio que permitirá comunicaciones a corta distancia con un elevado ancho de banda (del orden de 500 Mbps o superior). Sus aplicaciones pueden estar en la transmisión de vídeo y audio, la conexión entre dispositivos digitales (monitores, proyectores, cámaras de vídeo...)

Además las normas de auditorías y certificaciones relativas al sector seguirán evolucionando y adaptándose a los nuevos escenarios y necesidades de la tecnología. Uno de los puntos a tener en cuenta en un futuro cercano es la **evolución de la norma ISO 27001:2013**.

Capítulo 12

Anexos

12.1 Glosario de términos

A continuación se ofrecen, ordenadas alfabéticamente, unas breves definiciones de los términos que se han mencionado a lo largo de este proyecto.

ACL (Listas de Control de Acceso)

Si bien no forma parte de ningún estándar inalámbrico, la mayor parte de los productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la dirección *MAC* de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya *MAC* figura en la lista de control de acceso.

Ad-Hoc

Una red bajo topología Ad-Hoc consiste en un grupo de equipos que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso (AP). Las configuraciones Ad-Hoc son comunicaciones de tipo punto-a-punto. Los equipos inalámbricos necesitan configurar el mismo canal y SSID en modo "Ad-Hoc".

AES (Advanced Encryption Standard)

Sistema de cifrado conocido originalmente como Rijndael. Fue desarrollado por dos científicos belgas, Joan Daemen y Vincent Rijmen. El nuevo estándar es un cifrado de bloque simétrico que puede trabajar con claves de 128, 192 o incluso 256 bits.

AP (Access Point)

Dispositivo que transporta datos entre la red inalámbrica y la red cableada (infraestructura). Actúa como un concentrador para los usuarios de dispositivos inalámbricos. Se encarga de funciones como pueden ser filtrado, y seguridad. Su alcance depende de la gama de frecuencias utilizada.

Bluetooth

Estándar de comunicación inalámbrica que utiliza FHSS, capaz de transmitir a velocidades de 1 Mbps a una distancia de 10 metros entre aparatos (normalmente portátiles, impresoras, monitores, teclados, ratones, etc....) que implementen esta tecnología ya que su *FHSS/Hopping Pattern* es de 1600 veces por segundo, lo que asegura transmisiones altamente seguras. En cuanto a su implementación Bluetooth utiliza el término piconet. Un piconet es un grupo de 2 u 8 aparatos que utilizan Bluetooth que comparten el mismo rango que es utilizado por un *Hopping Sequence*, a su vez cada piconet contiene un aparato principal (*master*) que es el encargado de coordinar el *Hopping Pattern* del piconet para que los demás aparatos (*slaves*) sean capaces de recibir información.

CCMP (Counter Mode with CBC-MAC Protocol)

Protocolo complementario al TKIP basado en AES, cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

CHAP (Challenge Handshake Authentication Protocol)

Protocolo de autenticación para servidores PPP donde la contraseña no sólo se exige al empezar la conexión sino también durante la conexión, mucho más seguro que el PAP. Una vez efectuado el enlace, el servidor envía un mensaje de desafío al solicitante de la conexión, el cual responde con un valor hash que será comparado por el servidor con sus cálculos del valor hash esperado. Si el valor coincide, la autenticación prospera, de lo contrario, finaliza. En cualquier momento el servidor puede solicitar un mensaje de desafío. Debido a que los identificadores cambian frecuentemente y por qué la autenticación puede ser solicitada en cualquier momento.

CNAC (Closed Network Access Control)

Método mediante el cual sólo se permite el acceso a la red a aquellos que conocen previamente el nombre de la red, o SSID. Este nombre viene a actuar como contraseña.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

Es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente)

Distributed Coordination Function (DCF)

Método de acceso básico definido en el estándar MAC 802.11. Permite compartir automáticamente el medio entre varias estaciones que usen PHYs compatibles y CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) con *backoff* aleatorio.

DSSS (Direct-sequence spread spectrum)

Tecnología de transmisión usada en redes inalámbricas donde la señal de *data* en la estación de envío se combina con una secuencia de bits de mayor tasa de *data*, o código *chipping*, que divide los datos de usuario de acuerdo a un ratio en despliegue. El código *chipping* es un patrón de bits redundante para cada bit que se transmite, lo cual incrementa la resistencia de la señal a la interferencia. Si uno o más bits en el patrón sufren daños durante la transmisión, los datos originales pueden ser recuperados debido a la redundancia de la transmisión.

EAP (Extensible Authentication Protocol)

Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que

se incluyen tarjetas de identificación, contraseñas de un sólo uso, autenticación por clave pública mediante tarjetas inteligentes, certificados y otros. Junto con los métodos de autenticación EAP de alto nivel, es un componente tecnológico crítico para las conexiones seguras a través de una red privada virtual (VPN), puesto que ofrece mayor seguridad frente a ataques físicos o de diccionario y de investigación de contraseñas, que otros métodos de autenticación, como CHAP.

Firewall

Sistema de defensa basado en la instalación de una barrera entre una computadora, un punto de acceso o un router y la Red por la que circulan todos los datos. Este tráfico es autorizado o denegado por el firewall, siguiendo instrucciones previamente configuradas.

FHSS (Frequency Hopping Spread Spectrum)

Sistema de transmisión de datos en la capa física que divide los datos en paquetes de información que, por motivos de seguridad, para dificultar su interceptación por terceros, los envía a través de varias frecuencias (*Hopping Pattern*) seleccionadas al azar y que no se superponen entre sí, siempre dentro de la banda de los 2,4 GHz. Se reservan 83 MHz para FHSS.

IEEE (Institute of Electrical and Electronic Engineers)

Formado a fecha de julio de 2003 por 377.000 miembros en 150 países. Cuenta con 900 estándares activos y 700 en desarrollo (<http://www.ieee.org>).

IEEE802.X:

Conjunto de especificaciones de las redes LAN dictadas por el IEEE (*Institute of Electrical and Electronic Engineers*). La mayor parte de las redes cableadas cumplen la norma 802.3, especificación para las redes *ethernet* basadas en CSMA/CD, o la norma 802.5, especificación para las redes *Token Ring*. Existe un comité 802.11 trabajando en una normativa para redes inalámbricas de 1 y 2

Mbps. La norma tendrá una única capa MAC para las siguientes tecnologías: *Frequency Hopping Spread Spectrum* (FHSS), *Direct Sequence Spread Spectrum* (DSSS) e infrarrojos. Se están desarrollando borradores de las normas.

IEEE 802.1X

Utiliza el protocolo de autenticación extensible o EAP, para autenticar al dispositivo móvil, permitiendo a la Entidad de Autenticación de Puertos (*Port Authentication Entity*, PAE) un control del proceso de autenticación a la red.

Infraestructura de red

Red inalámbrica centrada en un punto de acceso. En este entorno los puntos de acceso no solo proporcionan comunicación con la red cableada sino que también median el tráfico de red en la vecindad inmediata.

IPSec (IP Security)

Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguro de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de cifrado: Transporte y Túnel. El primero sólo cifra la parte relativa a los de datos (*payload*) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, cifra todo.

LAN (Local Area Network)

Red informática que cubre un área relativamente pequeña (generalmente un edificio o grupo de edificios). La mayoría conecta puestos de trabajo y PCs. Cada nodo (ordenador individual) tiene su propia CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail)... Sus características son: Topología en anillo o lineal,

Arquitectura punto a punto o cliente/servidor, Conexión por fibra óptica, cable coaxial o entrelazado, ondas de radio.

LEAP (Lightweight Extensible Authentication Protocol)

Protocolo del tipo EAP patentado por Cisco basado en nombre de usuario y contraseña que se envía sin protección. Esta metodología descuida la protección de las credenciales durante la fase de autenticación del usuario con el servidor.

LOPD (Ley Orgánica de Protección de Datos)

La Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (BOE 14-12-1999), resulta de la aplicación a todos los datos de carácter personal, entendidos como “cualquier información concerniente a personas físicas identificadas e identificables”, que sean susceptibles de tratamiento automatizado (o no) en papel también se aplica, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Para “garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”, que constituye el objeto de la Ley, ésta recoge una serie de medidas de obligado cumplimiento para todas las empresas y entidades públicas que dispongan de bases o ficheros informáticos o en papel con datos de carácter personal.

MAC (Media Access Control Address)

Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexadecimal. En redes IEEE 802, la capa *Data Link Control* (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: *Logical Link Control* (LLC) y *Media Access Control* (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI, la dirección del nodo se denomina *Data Link Control* (DLC) *address*.

MS-CHAP (Challenge Handshake Authentication Protocol)

Protocolo de autenticación utilizado por el acceso remoto de Microsoft y conexiones de red y de acceso telefónico. Con CHAP los clientes de acceso remoto pueden enviar de forma segura sus credenciales de autenticación a un servidor de acceso remoto. Microsoft ha creado una variante de CHAP específica de Windows denominada MS-CHAP.

NAT (Network Address Translation)

Estándar de Internet que le permite a una red local (LAN) usar un grupo de direcciones de IP para el tráfico interno y otro grupo de direcciones para el tráfico externo. Una tabla de NAT ubicada donde la LAN se conecta a Internet hace todas las traducciones necesarias de IPs.

NLOS (Near Line of Sight)

Las tecnologías de radiofrecuencia utilizan el término NLOS para describir un trayecto parcialmente obstruido entre la ubicación del transmisor de la señal y la ubicación del receptor de la señal. Los obstáculos que pueden obstaculizar la línea de vista incluyen árboles, edificios, montañas y otras estructuras y/u objetos contruidos por el hombre u obra de la naturaleza.

OFDM (Orthogonal Frequency Division Multiplexing)

Técnica de modulación FDM (empleada por el 802.11a) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (*crosstalk*) en las transmisiones de señal.

OSA (Open System Authentication)

Es el mecanismo de autenticación por defecto para las redes 802.11, y permite que cualquier estación se una al sistema tras la negociación de los parámetros de red necesarios, es decir, se utiliza autenticación NULA, en la que cualquier dispositivo puede obtener acceso a la red, sin realizarse ninguna comprobación. Además, todas las tramas de gestión son enviadas sin ningún tipo de cifrado, incluso cuando se ha activado WEP.

PEAP (Protected Extensible Authentication Protocol)

Protocolo del tipo EAP desarrollado conjuntamente por Microsoft, RSA Security y Cisco para la transmisión de datos autenticados, incluso claves, sobre redes inalámbricas 802.11. Autentica clientes de red wifi empleando sólo certificados del lado servidor creando un túnel SSL/TLS cifrado entre el cliente y el servidor de autenticación. El túnel luego protege el resto de intercambios de autenticación de usuario.

PPP (Point-to-Point Protocol)

Protocolo de comunicaciones utilizado para transmitir datos de la red a través de las líneas telefónicas. Este tipo de conexión permite comunicar directamente con otros ordenadores de la red por medio de conexiones TCP/IP.

RADIUS (Remote Authentication Dial-In User Service)

Sistema de autenticación y *accounting* empleado por la mayoría de proveedores de servicios de Internet (ISPs) si bien no se trata de un estándar oficial. Cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP si es así.

SSH (Secure Socket Shell)

Es una interfaz de comandos basada en UNIX y un protocolo para acceder de forma segura a una máquina remota.

SSID (Service Set Identifier)

Clave alfanumérica de 32 caracteres que identifica exclusivamente a una LAN inalámbrica. A menudo se le refiere como el Nombre de Red. Es utilizado para prevenir el acceso a su LAN de equipos inalámbricos no autorizados. Para comunicarse, los dispositivos inalámbricos en la misma red deben ser configurados con el mismo SSID.

SSL (Secure Sockets Layer)

Es un protocolo desarrollado por *Netscape Communications Corporation* para dar seguridad a la transmisión de datos en transacciones comerciales en Internet. Utilizando la criptografía de clave pública, SSL provee autenticación del servidor, cifrado de datos, e integridad de los datos en las comunicaciones cliente/servidor.

Términos de radio frecuencia: GHz, MHz, Hz.

La unidad internacional de medida de frecuencia es el Hertzio (Hz) el cual es equivalente a la unidad antigua de ciclos por segundo. Un MHz es un millón de Hertzios y un GHz son mil MHz (mil millones de Hz). Como referencia: La frecuencia eléctrica utilizada en Europa son 50 Hz y en EEUU son 60 Hz. La banda de frecuencia de radiodifusión AM es 0.55 - 1.6 MHz. La banda de frecuencia de radiodifusión FM es 88 - 108 MHz. Los hornos microondas típicamente operan a 2,45 GHz.

TKIP (Temporal Key Integrity Protocol)

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP, este protocolo posee un código de integración de mensajes (MIC) el cual cifra el *checksum* incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11 protegiendo con esto cualquier ataque por falsificación.

TTLS (Tunneles Transport Layer Security)

Protocolo de seguridad para redes inalámbricas del tipo EAP propiedad de la multinacional norteamericana Funk Software. Se trata de una extensión de EAP-TLS, protocolo utilizado por Windows XP en sistemas inalámbricos que proporciona los servicios de autenticación entre los usuarios y el servidor de la red basados en certificados. EAP-TTLS sólo requiere certificados al servidor, lo que subsana una desventaja importante respecto a EAP-TLS, cuya gestión es mucho más tediosa y pesada. Con EAP-TTLS se elimina la necesidad de configurar certificados para cada cliente de la red inalámbrica. Además, EAP-TTLS autentica al cliente en el sistema con las credenciales ya existentes basadas en password, y cifra credenciales y password para garantizar la protección de la comunicación inalámbrica.

VLAN

Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.

VPN (Virtual Private Network)

Sistema para simular una red privada sobre una pública. La idea es que la red pública sea vista desde dentro de la red privada como un “cable lógico” que une dos o más redes que pertenecen a la red privada. Para establecer este tipo de red, la integridad de los datos y la confidencialidad se protegen mediante la autenticación y el cifrado. Por ejemplo, los datos se pueden transmitir de forma segura entre dos sucursales a través de Internet o cifrarse entre un servidor y un cliente en una Red de área local (LAN).

WAN

Tipo de red compuesta por dos o más redes de área local (LANs) conectadas entre sí vía teléfono (generalmente digital).

Warchalking

Es la práctica de dibujar en paredes o aceras una serie de símbolos para indicar a otros la proximidad de un acceso inalámbrico.

Wardriving

Técnica difundida donde individuos equipados con material apropiado (dispositivo inalámbrico, antena, software de rastreo y unidad GPS) tratan de localizar en coche puntos *wireless*. Existen otras modalidades dependiendo de cómo se realice el rastreo: a pie, bicicleta, patines, etc...

WEP (Wired Equivalent Privacy)

Protocolo para la transmisión de datos "segura". Utiliza una clave secreta, utilizada para el cifrado de los paquetes antes de su retransmisión. El cifrado puede ser ajustado a 128 bits, 64 bits o deshabilitado. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la clave de cifrado. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

WIFI (Wireless Fidelity)

Nombre comercial con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.

WIMAX

Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio.

WPA (Wi-Fi Protected Access)

Estándar Wi-Fi, aprobado en abril de 2003, desarrollado para mejorar las características de seguridad del estándar WEP y permitir su implementación en productos inalámbricos que actualmente soportan WEP, pero la tecnología incluye dos mejoras con respecto a este último: emplea el protocolo de integridad de claves TKIP para codificar los datos e implementa el estándar 802.1x utilizando el protocolo de autenticación extensible (EAP) para la autenticación de usuarios.

WPA2 (Wi-Fi Protected Access 2)

Aprobado por la Wi-Fi Alliance (1 de Septiembre del 2004), basado en el estándar de seguridad para 802.11, 802.11i cumpliendo con las normas del *National Institute of Standards and Technology* (NIST) FIPS 140-2. WPA2 implementa el algoritmo AES a diferencia de WPA que utiliza RC4, sin embargo WPA2 es totalmente compatible con WPA.

12.2 Bibliografía

Para citar la bibliografía se han seguido las recomendaciones de la Biblioteca de la Universidad Carlos III, que a su vez se basan en las normas ISO 690-1987 para documentos escritos y la norma ISO 690-2 para documentos electrónicos.

Las normas se pueden encontrar en la siguiente dirección:

http://www.uc3m.es/portal/page/portal/biblioteca/aprende_usar/como_citar_bibliografia

Por lo que para este proyecto la estructura seguida de documentos escritos tiene la forma:

APELLIDO(S), Nombre. Título del libro. Edición. ISBN

Para documentos electrónicos se han estructurado de la siguiente manera:

Autor (Fecha). Título del documento [descripción del formato]. Disponible en: dirección de la página web. Fecha de consulta.

Bibliografía utilizada como referencia:

- Cisco Networking Academy. Fundamentos de redes inalámbricas. ISBN 84-8322-287-6
- Gast, Matthew. 802.11 Wireless Networks: The Definitive Guide, Second Edition. ISBN 978-0-596-10052-0
- Huidobro, Jose Manuel; Blanco Solsona, Antonio; Jordán Calero, Julia. Redes de área local: administración de sistemas informáticos. ISBN 8497324897
- Potter, Bruce. Fleck Bob. 802.11 Security. ISBN 978-0-596-00290-9
- Stalling, William. Fundamentos de seguridad en redes. Aplicaciones y Estándares. ISBN 84-205-4002-1

Bibliografía en formato electrónico:

- A fondo ZigBee [Artículo WEB].

Disponible en: <http://www.domodesk.com/a-fondo-zigbee>

Fecha de consulta: Diciembre 2013.

- Apuntes asignatura Auditoría Informática. Universidad Carlos III de Madrid
- Ardita, Julio Cesar. 2008. Análisis de WPA/WPA2 vs WEP. Escuela politécnica del ejército del Ecuador [PDF].

Disponible en: http://www.cybsec.com/upload/ESPE_Analisis_WPA_WEP.pdf

Fecha de consulta: Junio 2014.

- Cervera Tortosa, Carlos. 2005. Seguridad en Redes Inalámbricas. Departamento de informática. Universidad de Valencia
- El portal de ISO 27001 en Español

Disponible en: <http://www.iso27000.es/certificacion.html>

Fecha de consulta: Mayo/Junio-2015.

- Escudero Pascual, Alberto. 2007. Seguridad en Redes Inalámbricas
- Guía de desarrollo para Android

Disponible en: <http://developer.android.com/guide/index.html>

Fecha de consulta: 2014-2015.

- Kosutic, Dejan. Lista de apoyo para implementación de ISO 27001

Disponible en: <http://www.iso27001standard.com/es/blog/2010/09/28/lista-de-apoyo-para-implementacion-de-iso-27001/>

Fecha de consulta: Mayo-2015.

- Panda Software. 2005. Seguridad en redes inalámbricas [PDF].

Disponible en: http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf

Fecha de consulta: Mayo 2014.

- Martínez Martínez, Evelio. 2002. Estándares WLAN [Artículo WEB].

Disponible en: <http://www.eveliux.com/mx/Estandares-WLAN.html>

Fecha de consulta: Mayo 2014.

- Norma ISO 27001

Disponible en: <https://trabajoscun.wordpress.com/category/auditoria-de-sistemas/>

Fecha de consulta: Mayo/Junio-2015.

- Valle Islas, L. F. 2005. Coexistencia de Redes WLAN & WPAN. Tesis Licenciatura. Ingeniería en Electrónica y Comunicaciones. Departamento de Ingeniería Electrónica, Escuela de Ingeniería, Universidad de las Américas Puebla.